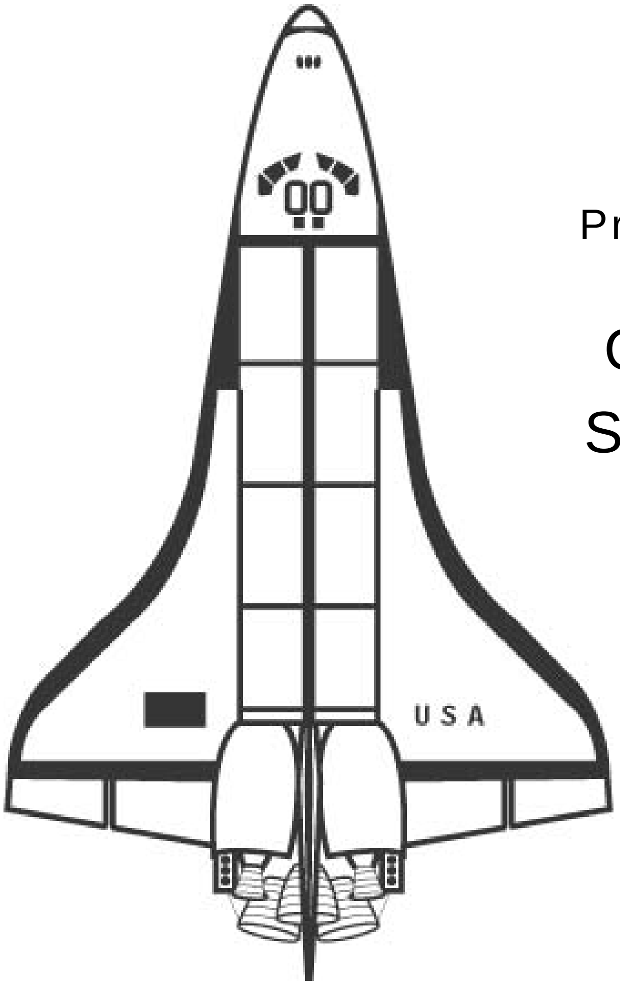
National Aeronautics and
Space Administration

NASA/Navy Benchmarking Exchange (NNBE)

Volume III

Progress Report | October 22, 2004

Ongoing NNBE Activities & Software Subgroup Report I



NNBE Benchmarking Team

**NASA Office of Safety &
Mission Assurance**

**NAVSEA 07Q Submarine Safety
& Quality Assurance Division**

This page intentionally blank.

Acknowledgement

The NASA/Navy Benchmarking Exchange (NNBE) Team gratefully acknowledges the cooperation and outstanding support of the Naval Sea Systems Command Submarine Safety (NAVSEA SUBSAFE) program management, as well as NASA and Space Shuttle program management. We especially want to thank the people of the Kennedy and Johnson Space Centers who hosted and supported visits by the NNBE Software Team, providing invaluable insight into NASA's software systems as the Navy enters into a new era of using remote computer control for activation of critical systems.

As NASA continues to focus on safety in its return-to-flight efforts, we particularly appreciate the support and openness of NAVSEA's participation in the Submarine Safety Colloquium to the newly established NASA Engineering and Safety Center, the Space Shuttle Program (SSP), the International Space Station (ISS), and other NASA programs. We are also grateful to the Pearl Harbor Naval Shipyard and Intermediate Maintenance Facility (PHNSY&IMF), as well as the SUBSAFE, Deep Submergence Systems, and Non-destructive Test and Evaluation teams for allowing the NASA representatives to observe their functional audits. The NNBE Team was also fortunate to have participated in the "Challenger Launch Decision" training provided by Knolls Atomic Power Laboratory (KAPL). This training opportunity provided the basis for the NASA Safety Critical Decision Making training initiative developed by the NASA Office of Safety and Mission Assurance and implemented by the NASA Academy of Program and Project Leadership.

The NNBE effort continues to foster the sharing of safety and mission assurance knowledge, expertise, and best practices of NASA and NAVSEA, formalized through the establishment of various Memoranda of Agreement that will provide continued access to valuable resources between our organizations. Through this exchange, we have discovered similarities in our experiences and in the challenges facing our organizations. We anticipate that this exchange will continue to serve as a basis for further knowledge sharing and continuing growth in the relationship between our communities.

This page intentionally blank.

Signature Page

The undersigned participated in developing the content and verifying the accuracy of the information presented in this Progress Report and the comparisons provided in section 3.3. The opportunities summarized in sections 2.7 and 3.3 represent the individual consensus of the NASA and NAVSEA core benchmarking teams.

NASA Team Lead

J Steven Newman

Dr. J. Steven Newman
Independent Assessment Team Lead
Office of Safety & Mission Assurance

NAVSEA Team Lead

A. H. Ford, Jr.

Mr. A. H. Ford, Jr., PE
Deputy Director, Submarine Safety & Quality Assurance
Naval Sea Systems Command (NAVSEA 07Q)

NASA Software Lead

Ms. Martha Wetherholt
Safety Assurance Requirements Division
Office of Safety & Mission Assurance

NAVSEA Software Lead

Mr. John A. Charles
Assistant Development & Modernization Manager (This position was titled "Assistant Research & Development Manager" at the time of the activities described in this report.)
VIRGINIA Class Submarine Program Office (NAVSEA PMS450)

This page intentionally blank.

Executive Summary

The NASA/Navy Benchmarking Exchange (NNBE) was initiated in August 2002 to share lessons learned on safety and mission assurance (SMA) policies, processes, accountability practices, and control measures in the Navy's submarine and NASA's human space flight programs. The exchange is a multi-phase effort, with the focus of this NNBE Report on Software Safety and Assurance in both NASA's Space Shuttle Program and the Navy's new VIRGINIA Class Ship Control System. The focus of Volume I was the Navy Submarine Safety Program (SUBSAFE) and the focus of Volume II was Naval Reactors Safety Assurance and the Naval Nuclear Propulsion Program (NNPP).

Significant progress has been made on efforts to implement a Safety Critical Decision Making Training Initiative, with multiple training classes offered and a roadmap for implementation in near-final form. Additionally, Memoranda of Agreement (MOA) for Product Quality Assurance and Engineering Investigations and Analyses have been signed and a Reciprocal Review of Audits agreement has been drafted. The NNBE also supported the NASA Engineering and Safety Center (NESC), an independent organization chartered in the wake of the Space Shuttle Columbia accident to serve as an Agency-wide technical resource focused on engineering excellence. Several sessions were held between selected senior NESC management members and Naval Sea Systems Command (NAVSEA) to provide insight into the Navy's Submarine Safety, Quality Assurance, Technical Authority and Independent Assessment / Compliance Verification best practices. Finally, the first Submarine Safety Colloquium was successfully completed in October 2003 to provide several groups within NASA insight into the Navy's submarine practices.

The Software Subgroup Report presents an initial report of NNBE findings for software safety and mission assurance, highlighting observations and opportunities derived from meetings at the NASA Independent Verification and Validation (IV&V) Facility in Fairmont, West Virginia and the Kennedy and Johnson Space Centers. NASA opportunities identified at these meetings include:

- Reappraising software implementation on the Space Shuttle Program (SSP) on both the contractor and civil servant sides using the Capability Maturity Model (CMM) to verify that their exemplary rigor has not diminished. This is especially important since the Shuttle is still certified at CMM Level 5 despite not having been appraised in 8 years, during which time it has changed contractors twice.
- Strengthening NASA's levels of defense for Assuring Software Safety and Quality. Specifically, this opportunity includes establishing and implementing better contractor requirements (Level 1), bolstering the Agency's Software Assurance resource pool (Level 2), and ensuring that IV&V is called upon only in critical situations (Level 3).
- Strengthening Agency CMM/CMMI related requirements for mission critical software. Some of this work has already been initiated in NASA SWE NPR 7150.2 (Software Engineering Requirements), which was in the administrative review cycle at the time of this report.

- Instituting IV&V software inspection efforts Agency-wide.

Navy opportunities identified at these meetings include:

- Developing a Centralized NAVSEA Software IV&V Organization
- Formalizing Software Development as a Warranted Technical Discipline at NAVSEA HQ
- Revising and Implementing NAVSEA-wide Software Standards
- Integrating Navy Laboratory Software Development into Lead Design Yard Efforts
- Performing Formal Causal Analysis on Software Deficiency Reports
- Reviewing the Shuttle Life Extension Program (SLEP) for lessons learned on extending the useful life of software
- Pursuing NASA Software Assurance Audit and Independent Assessment Lessons Learned
- Exchanging NASA/Navy Hardware/Software Information and Certification Processes for Commercial Off-the-Shelf (COTS) software.
- Considering a Test-oriented Design Language Similar to NASA's GOALS
- Considering Alternative Selection Criteria for software vendors

Next steps for the NNBE Team include plans to review software safety and mission assurance policies for the International Space Station (ISS) and to observe a SUBSAFE Certification Audit. Other topics will include Risk Management, Material Control, Work and Configuration Management, Personnel Management, and Design Tools/Techniques.

Table of Contents

Acknowledgement i
Signature Page iii
Executive Summary v
Table of Contents vii
List of Figures viii
List of Tables viii

1.0 Introduction and Scope 1

1.1 Background 1
1.2 Scope 1
1.3 Follow-on Activities 2

2.0 Progress on Key NNBE Initiatives 5

2.1 Safety Critical Decision Making 5
2.2 NASA/NAVSEA Product Quality Assurance Memorandum of Agreement 8
2.3 NASA/NAVSEA Engineering Investigations & Analyses Memoranda of Agreement 10
2.4 NASA/NAVSEA Reciprocal Review of Audits Memoranda of Agreement 11
2.5 NASA Engineering & Safety Center (NESC) Support 12
2.6 Submarine Safety Colloquium (SSC) 14
2.7 Pearl Harbor Naval Shipyard & Intermediate Maintenance Facility Audit 17

3.0 Software Subgroup Report I 21

3.1 NASA Software Development & Safety - Summaries and Key Observations 22
3.1.1 Organization (NASA) 22
3.1.2 Software Safety Requirements (NASA) 30
3.1.3 Implementation Processes (NASA) 34
3.1.4 Compliance Verification Processes (NASA) 40
3.1.5 Certification Processes (NASA) 44

3.2 Navy Software Development & Safety - Summaries and Key Observations 47
3.2.1 Organization (Navy) 47
3.2.2 Software Safety Requirements (Navy) 54
3.2.3 Implementation Processes (Navy) 60
3.2.4 Compliance Verification Processes (Navy) 66
3.2.5 Certification Processes (Navy) 71

3.3 Comparative Context & Opportunities 72
3.3.1 Comparative Context 72
3.3.2 Opportunities 74

APPENDIX A: Software Subgroup Report I – Key Observations.. 81
Appendix A-1: NASA – Summary of Key Observations... 81
Appendix A-2: Navy – Summary of Key Observations.. 85

APPENDIX B: Elements of Safety Critical Decision Making Initiative Plan....................... 89
Appendix B-1: Agency All-Hands 93
Appendix B-2: Senior Leadership Seminar... 94
Appendix B-3: Senior Management Workshop... 97
Appendix B-4: Program/Project Team Workshop... 101

APPENDIX C: NNBE Memoranda of Agreement (MOA) 105
Appendix C-1: Quality Assurance Agreement.. 105
Appendix C-2: Engineering Investigations and Analyses Agreement 111

APPENDIX D: Navy Memos outlining Software Safety Criteria....................................... 115
Appendix D-1: Seawolf Class Software Safety Criteria.. 115
Appendix D-2: Virginia Class Software Safety Criteria 119

Glossary 129

Referenced Documents 134

List of Figures

Figure 1. CAIB Observations on NASA’s Safety Culture. 5
Figure 2. NASA/NAVSEA Product Quality Agreement.. 9
Figure 3. NASA/NAVSEA Engineering Investigations and Analyses Agreement.................... 10
Figure 4. Submarine Safety Colloquium. 14
Figure 5. NASA Organizational Structure... 24
Figure 6. Shuttle Software Projects. 28
Figure 7. Hazard Severity Definitions. 34
Figure 8. Software Safety Litmus Test Example.. 35
Figure 9. Software Assurance Umbrella.. 45
Figure 10. Organizations that Comprise Team Submarine.. 49
Figure 11. PMS 450 Organization. 50
Figure 12. Virginia Class Ship Control System Software Safety Criteria.................................. 57

List of Tables

Table 1. Safe Critical Decision Making Course Statistics... 7
Table 2. SUBSAFE/DSS Functional Audit Findings 18
Table 3. PMS 450 Roles & Responsibilities in the Software Management Process 48

NASA/NAVY Benchmarking Exchange (NNBE) Progress Report, Volume III

1.0 Introduction and Scope

1.1 Background

The NASA/Navy Benchmarking Exchange (NNBE) was undertaken to identify practices and procedures and to share lessons learned from both the Navy's submarine and NASA's human space flight programs. Initiated in August 2002, the NNBE focus is on safety and mission assurance (SMA) policies, processes, accountability practices, and control measures. The benchmarking exchange has been divided into a multi-phase effort consisting of NASA's review of Navy practices and procedures and the Navy's review of NASA space flight SMA processes.

An interim report summarizing the initial activities completed through October 2002 was prepared and presented to the NASA Administrator on December 20, 2002. The focus of Volume I was the Navy Submarine Safety Program (SUBSAFE). A second report summarizing NNBE progress through June 2003 was provided to the Administrator on July 15, 2003. The focus of Volume II was Naval Reactors Safety Assurance and the Naval Nuclear Propulsion Program (NNPP). Both Volumes I and II concentrated on the themes of new design/construction and maintenance/modernization while employing a benchmarking framework that addressed:

1) Management and Organization,
2) Safety Requirements (technical and administrative),
3) Implementation Processes,
4) Compliance Verification Processes, and
5) Certification Processes.

1.2 Scope

The focus of this NNBE Progress Report is Software Safety and Assurance within NASA's Space Shuttle Program and the Navy's VIRGINIA and SEAWOLF Class Ship Control Systems as well as the Advanced Seal Delivery System. A NNBE splinter group was formed specifically to address software, and the initial findings and progress to date are presented in Section 3 of this document, with Key Observations for both Navy and NASA software safety and assurance summarized in Appendix A. This report marks the first time the NNBE has compiled observations and opportunities for both NASA and Navy programs.

Section 2 of this document summarizes progress on several key NNBE initiatives, including:

- NASA efforts to implement a Safety Critical Decision Making Training Initiative,
- Status of NNBE Memoranda of Agreement (MOA) between NASA and the Navy,
- NNBE support to the NASA Engineering and Safety Center (NESC),
- The first-ever Submarine Safety Colloquium held in October 2003, and
- NASA NNBE participation in the Navy's functional audit process.

1.3 Follow-on Activities

Future NASA review activities include potential NASA observation of Naval Sea Systems Command (NAVSEA) certification audits for both new construction and submarines completing a major availability depot maintenance period. It is anticipated that these will be completed in the fall of 2004 as specific opportunities become available. Other potential NASA NNBE technical interchange topics include:

- Deep Submergence Systems,
- Affordability Initiatives,
- Concept Development/Technology Infusion, and
- The Role of NAVSEA Senior Management in the Certification Process.

Potential new topics for NNBE discussions on software have been identified, including software assurance practices for International Space Station (ISS) and Naval Reactors. These events are expected to occur as NAVSEA's schedule permits relative to delivery and construction of VIRGINIA Class submarines.

Previously planned NAVSEA review activities on hold as NASA completes its return to flight efforts include:

- Follow-on Site Visit to Kennedy Space Center (KSC),
  (SME splinter groups, Shuttle ground operations, Software design, development, and assurance programs, KSC industrial safety, cranes, pre-launch certification of the Shuttle)
- Follow-on Site Visit to Johnson Space Center (JSC),
  (JSC roles and responsibilities, SMA roles of government, Software design, development, and assurance programs, structural inspection, upgrades/life extension, and other special topics)
- Site Visit to Michoud Assembly Facility and Stennis Space Center,
  (Observe critical process management, NDE processes, advanced welding processes, weld and weld repair processes, SSME Testing / Certification processes)
- Site Visit to Thiokol Space Shuttle Solid Rocket Motor Facility,
  (Facility orientation/briefings, critical process management approaches, process fail-safing, supply chain management, risk management, etc.)
- Site Visit to Ames Research Center,
  (Human Factors, fatigue countermeasures, human error countermeasures, NASA man-system integration standard, human rating requirements, human modeling, HF FMEA, ergonomics and lifting analysis, and HF in mishap investigation)
- Observation of a NASA Engineering and Quality Audit (NEQA), and
- Participation in NASA Risk Management Colloquia.

Software Development & Safety

Additional Navy and NASA review activities have yet to be completed. The Navy plans to review software safety and mission assurance policies for the International Space Station (ISS). Both the VIRGINIA Class submarine and the ISS have made extensive use of Commercial Off-the-Shelf (COTS) software, and the Navy feels it would benefit from experiences and lessons learned from the ISS program.

NASA has expressed interest in other software systems on the VIRGINIA Class submarine. While the Ship Control System was discussed extensively in the previous meetings, time did not permit discussion of other critical software programs on the VIRGINIA Class. It is proposed that software development and software safety analyses be the subject of targeted discussion with Naval Reactors, including both NASA and NAVSEA personnel.

The largest software developments at NAVSEA are accomplished by those systems which are part of the Command, Control, Communications and Intelligence (C3I) systems. The submarine-related programs are as significant in size, complexity and capability as any in the Navy. While not SUBSAFE programs, these systems do support safe operation of the submarine. General discussion on software development practices with appropriate NAVSEA organizations and their prime contractors could provide NASA with insight into mature software development practices. Similar discussions might also be of value with those Navy organizations responsible for weapons system development, and would include discussion of the Navy's Weapon System Explosives Safety Review Board (WSESRB) process.

With the recent codification of requirements for fly-by-wire (FBW) submarine ship control systems, there is an opportunity for targeted discussion of the process, product, and organizational changes implemented by the Navy in accordance with the NAVSEA T9044-AD-MAN-010 "Requirements Manual for Submarine Fly-by-Wire Ship Control Systems." A presentation by the Navy of the implementation of the Requirements Manual is a primary candidate for further software discussion.

In addition, both NASA and the Navy would like to extend discussions beyond the limited exchanges that took place during previous two meetings. Topics to be considered at a future date include the following software related topics:

- Risk Management,
- Material Control,
- Configuration Management,
- Personnel Management / Training,
- Work Management,
- Design Tools / Techniques, and
- Certification Audits / Review Process.

This page intentionally blank.

2.0 Progress on Key NNBE Initiatives

2.1 Safety Critical Decision Making

As a result of early NNBE exchanges, NASA has implemented a Safety Critical Decision Making (SCDM) training program based on the Knolls Atomic Power Laboratory's safety critical decision training program for NAVSEA's Naval Nuclear Propulsion organization (Naval Reactors). This program includes a 3-hour seminar about the Challenger Launch Decision and the events, communications, and discussions that led to the decision to launch the Space Shuttle Challenger in January of 1986. As a result of NNBE activities, NASA representatives from the Administrator's Office, the Office of Safety & Mission Assurance, Space Operations, Human Resources, and Kennedy, Marshall, and Johnson Space Centers attended the Challenger Decision Training course in May 2003 and overwhelmingly supported the notion of developing a similar course for NASA.

Chapters 7 and 8 of the CAIB Report discuss NASA safety cultural shortcomings. The Stafford/Covey team is addressing what the NASA safety culture is and what measures are underway to address perceived shortcomings and multiple Space Shuttle Program (SSP) and Return to Flight (RTF) teams are addressing various aspects of "safety culture." The SCDM training program provides the following specific responses to CAIB observations:

- Responds to CAIB Report recommendation R6.3-1: "Implement an expanded training program" (Section 6.3) – (Mission Management Team focus - Missed Opportunities)
- Implicitly addresses concerns expressed in Section 7.4: "A Broken Safety Culture"
- Complements Observation 10.12-1 "Implement an Agency wide strategy for leadership and management training … " (Section 10.12) - (Leadership/Managerial Training)
- Implicitly addresses concerns expressed in Section 8.2, "Failure of Foresight" – "Normalization of Deviance" – "In Family Concept"
- Implements "Best Safety Practices" cited in CAIB section 7.3:
    - "Recurring Training & Learning from Mistakes" –Navy Submarine and Reactor Safety Programs
    - "Encouraging Minority Opinions"

Figure 1. CAIB Observations on NASA's Safety Culture.

The NASA Office of Safety & Mission Assurance-based NNBE Management Team has worked closely with NAVSEA and the NASA Academy of Program and Project Leadership (APPL) in the Office of the Chief Engineer to develop a course concept and plan for Safety Critical Decision Making (SCDM).

This NASA-wide initiative uses the Naval Reactors (NR) workshop as a cornerstone, placing emphasis on the role and responsibility that every member of the NASA team, both civil service and contractor, has regarding the quality, safety, and success of NASA's missions, and reinforcing that emphasis on a regular basis. This initiative provides sustained and adaptive training relevant to all NASA employees with specific focus for senior management and program/project teams.

The Office of Safety and Mission Assurance (OSMA), in partnership with APPL, has developed a program implementation plan for institutionalizing this course material into a four-part SCDM training initiative. This plan has been presented to the Chief Engineer, the Associate Administrator for Safety and Mission Assurance, the Director of Personnel, and the Associate Deputy Administrator for Technical Programs and has subsequently been modified to reflect their review.

Options of the initiative include (1) an Agency All Hands presentation to all NASA staff and contractors, (2) a Senior Leadership Seminar, (3) Senior Management Workshops, and (4) decision-making workshops designed for program/project teams. Detailed outlines of each of these four elements are provided in **Appendix B.** Proposed curricula for each of the four fundamental training events have been drafted and pilot versions of the senior management workshop have been conducted at the JSC, KSC, Marshall Space Flight Center (MSFC), Headquarters (HQ), and the Senior Leadership Seminar at the NESC. [1] The pilots have been continually updated to incorporate comments from the student participants and to include Columbia findings as well as Tufte aspects.

Next steps include:

1. Presenting an overview of the Safety Critical Decision Making content and the implementation approach to the Administrator’s Senior Staff.

2. Involving other Enterprise and functional office representatives as well as the Space Shuttle Program Return to Flight (SSP RTF) in a steering group/management team as the initiative evolves, including briefing the proposal to the RTF Space Flight Leadership Council.

3. Kicking off the Safety Critical Decision Making (SCDM) initiative with a one-hour Agency “All Hands” presentation (**Appendix B-1**) that will highlight NASA’s past decision process and the importance of critical decision-making, and inaugurate the roll-out of decision-making culture change.

4. Conducting half-day Senior Leadership Workshops (**Appendix B-2**) to engage Senior Leaders in key aspects of the critical decision training. As lynch-pins of the cultural change process, their ability to motivate their organizations and to drive home the significance of the training will be critical.

5. Continue to conduct the Senior Leadership Workshop—two day Senior Management Workshops—facilitated sessions attended by members of the senior staff. The subject will be “Critical Decision Making for Executives” (**Appendix B-3**).

[1] A pilot Senior Management Workshop was held at JSC for the RTF Manned Mission Team (MMT) the first week in March, 2004, and was very well received. Additionally, pilots were conducted at KSC and MSFC with similar results, and presentation of the 2 day course is now booked at JSC through the end of 2004.

6. Involving Program/Project teams in three-day facilitated workshops (**Appendix B-4**) that explore NASA's culture, group decision-making techniques and considerations, and individual roles and accountability. The course will include guest speakers, case studies, and participatory problem solving exercises.

Detailed implementation will be directed by APPL, providing tailored curricula suitable for all levels of NASA employees (senior management, program and project managers, and administrative staff).

Table 1. Safety Critical Decision Making Course Statistics

(as of 9/10/2004)

Course	Location	# of Times Presented	Attendees
1.5 day managers course	JSC	2	24 each
	KSC	1	24
	MSFC	1	24
	HQ	1	15
4 hour course	NESC	1	35
2 day course (Expansion of the 1.5 day course requested by previous participants)	JSC	2	24 each
	JSC	1 planned for Dec. 2004	24
	JSC	TBD	24
	MSFC	Q205	24
	OSMA	15-20	TBD

Note: Program write-ups were sent to all SMOs and Training Offices at the other seven NASA Centers

2.2 NASA/NAVSEA Product Quality Assurance Memorandum of Agreement

In keeping with the collaborative spirit of the initial agreement between the Navy and NASA, a series of Memoranda of Agreement have been established for the sharing of information, procedures, and data for potential application to each organization's programs and projects. The first MOA, signed on June 26, 2003, was between the United States Navy Naval Sea Logistics Center Detachment (NAVSEALOGCENDET) Portsmouth, NH and NASA's Office of Safety and Mission Assurance (OSMA) in Washington, DC.

This is an agreement for NASA to use the Navy's web-accessible Product Data, Reporting, and Evaluation Program (PDREP), and the web-accessible Red/Yellow/Green (RYG) Program described in the NNBE's Interim report (Volume I) of December 20, 2002. These two programs will be used as secure repositories of proprietary data on NASA Contractors as well as a source of data on potential contractors during the acquisition process.

<u>PDREP Program</u>

The PDREP is an automated information system designed to track quality and delivery performance on material/services procured by the Navy. Data is collected from all Naval Systems Commands on a daily basis and is maintained in the following records on the database:

- Contractor Name
- CAGE Information
- Debarment/Suspension
- Contract Delivery Data
- DLA Contractor Alert List
- GIDEP Alerts
- Material Inspection Records
- Product Quality Deficiency Reports
- Qualified Product List
- Special Quality Data
- Surveys
- Test Reports

PDREP offers a wide selection of standard, management, and graphical reports as well as allowing users to design their own reports. The Feedback function of PDREP also provides users the opportunity to request modifications to reports or to make suggestions that would enhance any NAVSEALOGCEN application/program. The Feedback site then assigns the appropriate knowledge expert for completion/resolution.

<u>Red/Yellow/Green (RYG) Program</u>

The RYG Program is a Navy/Air Force automated tool designed to help reduce the risk of the government receiving nonconforming products and late shipments. RYG classifies the risk degree by assigning a color to a contractor's historical quality and delivery performance in individual Federal Stock Classifications (FSCs). Red is high risk, yellow is moderate risk, and green is low risk. A neutral label is applied to the quality/delivery classification of the FSC if:

- contractor is a first-time offeror,
- no quality/delivery history is available, or
- available quality/delivery history is outside the RYG evaluation time frame.

> The Logistics Center acts as a clearinghouse with little or no input into the supporting data. Each Vendor is notified of its commodity grade, in detail down to line item number, and is allowed to challenge or verify within 30 days.

The MOA states that:

> *"NAVSEALOGCENDET Portsmouth will provide NASA with web-access to the PDREP Automated Information System (AIS) to store NASA product quality information, and the RYG program to store delivery data. NASA will have use of both programs per the terms of this agreement. These web-based tools will enhance the ability of NASA, agency-wide, to assess contractor performance history and contractor ability to deliver high quality products on time and within budget. This will be especially helpful in assuring NASA's timely and accurate evaluation of contractor proposals for both hardware and services and will enhance NASA's ability to select only the best for the Nation's procurements of critical systems for human exploration of space.*
>
> *"Correspondingly, this agreement makes NASA Contractor information available to the Navy in their procurements and will provide a similar expansion of contractor performance knowledge in proposal evaluation and contractor selection."*

This ground-breaking agreement was the first in a series of agreements envisioned between NASA and the U.S. Navy for both organizations to identify and use the "best of the best" practices to improve safety, mission assurance, and performance of the systems procured by both. This MOA involves exchange of funds to support NASA's access to and application of these tools to NASA's evaluation of contractor performance.

Figure 2. NASA/NAVSEA Product Quality Agreement

Left: Bryan O'Connor (NASA) and Stephen Bonwich (NAVSEA) formalize the Product Quality Agreement.
Right: The NASA/NAVSEA Team who structured the Product Quality Agreement.

A full version of the signed agreement is provided in **Appendix C-1**.

2.3 NASA/NAVSEA Engineering Investigations & Analyses Memoranda of Agreement

Another MOA was established on December 2, 2003 between NASA's OSMA and the U.S. Navy's NAVSEA. This agreement provides reciprocal rights to participate in on-going or new engineering investigations and analyses of programs and projects.

Participation in investigations and analyses under the auspices of these agreements will be governed by program/project sensitivity and national security considerations and will be conducted solely at the discretion of the hosting organization.

The Engineering Investigations and Analyses Agreement

> *"provides NASA and its field activities, and NAVSEA and its field activities, reciprocal rights to participate in the conduct of mutually agreed, on-going or newly created engineering investigations and analyses of programs and projects. The participation by one Party in the other Party's programs/projects will be governed by the mission, sensitivity, security, safety, and national security considerations associated with that program/project and will be conducted solely at the invitation of the Party whose program/project is undergoing the engineering investigation analysis. The intent of this MOA is to allow each Party to participate in (contribute) and learn from the other Party's processes."*

This agreement is provided in its entirety in **Appendix C-2**.

Figure 3. NASA/NAVSEA Engineering Investigations and Analyses Agreement.

Gregg Hagedorn (NAVSEA) and Bryan O'Connor (NASA) formalize the Engineering Investigations & Analysis Agreement.

2.4 NASA/NAVSEA Reciprocal Review of Audits Memorandum of Agreement

The NNBE has been working on an additional MOA with NAVSEA relative to participation in audits. The content is similar to that of the agreement on Engineering Investigations. This MOA has undergone review by NASA legal counsel, is currently being reviewed within NAVSEA, and is pending signature.

2.5 NASA Engineering & Safety Center (NESC) Support

The NESC is an independent organization, chartered in the wake of the Space Shuttle Columbia accident to serve as an Agency-wide technical resource focused on engineering excellence. The objective of the NESC is to improve safety by performing in-depth independent engineering assessments, testing, and analysis to uncover technical vulnerabilities and to determine appropriate preventive and corrective actions for problems, trends, or issues within NASA's programs, projects and, institutions. The NESC draws upon the best engineering expertise from across the Agency and includes partnerships with other government agencies, national laboratories, universities, and industry.

On August 19, 2003, an initial meeting was conducted between selected senior NESC management members and NAVSEA to provide insight into the Navy's Submarine Safety, Quality Assurance, Technical Authority, and Independent Assessment / Compliance Verification best practices observed during the NNBE activities. Speakers at the meeting included the Deputy Director for Submarine Safety and Quality Assurance (NAVSEA 07Q) and the Ship Design Manager, Virginia Class Submarines (NAVSEA 05).

NAVSEA 07Q kicked off the meeting with films summarizing the USS THRESHER and USS SCORPION accidents. The USS Thresher sank in 8,500-foot deep waters with the loss of 112 navy personnel and 17 civilians on board in April, 1963. This accident was the impetus for the SUBSAFE program, created in June, 1963. While the USS Scorpion was lost in May 1968, it should be noted that this loss was not a SUBSAFE related accident. A detailed overview of the SUBSAFE program was presented, including discussions and Q&A on the following topics:

- SUBSAFE organization and personnel staffing
- Life-cycle responsibility of SUBSAFE program for contractors
- Technical Authority within the SUBSAFE program
- "Triangle" decision authority model (Safety vs. Requirements vs. Program)
- Downsizing
- NAVSEA technical warrants
- NAVSEA technical instructions
- Design certification process
- Initial ship certification process before going to sea
- Certification authority
- Certification package / Objective Quality Evidence (OQE)
- Functional and Certification Audits
- The SUBSAFE Oversight Committee
- Software and the SUBSAFE program
- Proposed Changes to the SUBSAFE program
- SUBSAFE and Trending Metrics

NAVSEA 05 presented a review of the newest submarine class, the VIRGINIA Class, including discussions and Q&A on the following topics:

- Virginia Class submarine capabilities and design
- “Fly-by-wire” technology – or use of remote computer control to activate systems
- Advanced Seal Delivery System: SUBSAFE vs. Deep Submergence System Requirements
- Contractor teaming arrangements relative to design/build
- Evolutionary design and Lessons Learned / Ship Specifications
- Streamlining the design process through use of
    - standard parts wherever possible
    - electronic design tools such as Catia
    - contractor team-sharing of design model / parts system
    - Commercial Off-the-Shelf (COTS) parts
    - parts obsolescence tracking in industry evolution: whether to stockpile parts or redesign with a new COTS part
- Design redundancy requirements / fault tolerance for critical systems
- Self-testing for hardware and software interfaces
- Independent assessments

This initial meeting was followed by a larger NAVSEA presentation to the NESC (see section 2.6, Submarine Safety Colloquium).

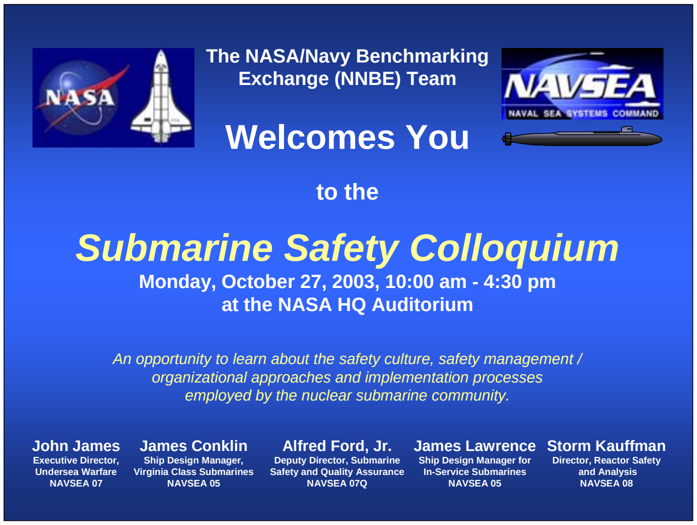
Next, on October 31, 2003, as part of the on-line collaboration (eGov) initially specified as part of the NNBE Management Team approach to data gathering/sharing, the NASA Office of Safety and Mission Assurance presented an overview briefing to the NESC. This briefing highlighted the benefits of the Process Based Mission Assurance Knowledge Management System (PBMA-KMS). In particular, the Knowledge Registry tool and the online collaborative environment Work Group tool were emphasized.

1. The Knowledge Registry tool (currently under development) is an on-line data repository of subject matter experts within NASA (and ultimately other government agencies and industry) that the NESC will be able to use to facilitate independent technical assessments.
2. On-line Work Groups allow NESC communities of practice to share files, calendars, action tracking, threaded discussions, etc.

Finally, on November 18-19, 2003, NESC representatives also attended the PBMA-KMS Communities of Practice III Workshop. NESC has requested and is actively using nineteen (19) PBMA online Work Groups to collaborate on problem resolution for topics ranging from Life Support, Thermal, and Fluid Systems, to Guidance, Navigation, and Control, to Human Space Flight Operations.

2.6 Submarine Safety Colloquium (SSC)

Following the first meeting between the NESC and the Navy in August 2003, it was decided that the full membership of the NESC should be exposed to the Navy's safety processes, practices, and tools. At the same time, in the aftermath of Columbia, several groups within NASA were working to respond to the then-recently-released Columbia Accident Investigation Board Report and preparing NASA to return to flight. In an effort to support all of these groups, the NNBE Team decided to conduct a Submarine Safety Colloquium to provide NASA insight into the Navy community.



The NASA/Navy Benchmarking Exchange (NNBE) Team

Welcomes You

to the

Submarine Safety Colloquium

Monday, October 27, 2003, 10:00 am - 4:30 pm
at the NASA HQ Auditorium

An opportunity to learn about the safety culture, safety management / organizational approaches and implementation processes employed by the nuclear submarine community.

John James
Executive Director,
Undersea Warfare
NAVSEA 07

James Conklin
Ship Design Manager,
Virginia Class Submarines
NAVSEA 05

Alfred Ford, Jr.
Deputy Director, Submarine
Safety and Quality Assurance
NAVSEA 07Q

James Lawrence
Ship Design Manager for
In-Service Submarines
NAVSEA 05

Storm Kauffman
Director, Reactor Safety
and Analysis
NAVSEA 08

Figure 4. Submarine Safety Colloquium.

The colloquium was held on October 27, 2003 in the NASA HQ Auditorium in consonance with the week of NESC Leadership Team Training in Washington, D.C.

Navy participants/presenters included:

- Executive Director, Undersea Warfare – NAVSEA 07
- Ship Design Manager, Virginia Class Submarines – NAVSEA 05
- Deputy Director, Submarine Safety and Quality Assurance – NAVSEA 07Q
- Ship Design Manager for In-service Submarines – NAVSEA 05
- Director, Reactor Safety and Analysis – NAVSEA 08, Naval Reactors

NASA Participants included representatives from each of the following organizations:

- NASA Engineering Safety Center (NESC)
- Space Shuttle Program – Return-to-Flight Planning Team
- Space Shuttle Program Office
- Return-to-Flight Task Group
- Orbital Space Plane Program Office
- NASA HQ Office of Safety and Mission Assurance
- NASA HQ Comptroller
- NASA Inspector General (HQ and KSC)

This was a one-time opportunity for a large number of NASA organizations to be made aware of the processes used by the Navy to assure the creation, deployment, and support of a fleet of highly complex, tightly coupled systems for periods of 20 years and beyond. Highlights from five presentations are shown below.

1. General Remarks from the Executive Director for Undersea Warfare
   - The Director emphasized that "who holds the job matters," the importance of absolute and unwavering rigor in configuration management, and the need to do the "systems look" at any technical problem.

2. The World of Submarines, presented by the Ship Design Manager for the VIRGINIA Class Submarine
   - This presentation contained descriptive material on the construction of a submarine and its components, how the submarine program is structured and managed at the top levels, the process of an evolving system of ship specifications that incorporates lessons learned for each generation of submarine, and the necessity of full concurrence of all participants.
   - The presentation highlighted that the Ship Design Manager is the driver for ensuring lessons learned are transferred to the specifications and maintaining the legacy of high quality, safety, and reliability.
   - It also highlighted that lessons learned come from active day-to-day fleet message traffic, ship alteration documentation, general overhaul compendia, CASREP (Casualty Report) records, and INSURV (Board of Inspection and Survey) records. The lessons learned are conveyed in Design Decision Memoranda from NAVSEA HQ to the Supervisor of Shipbuilding (SUPSHIPS) to the Design Yards.
   - The Ship Design Manager noted the three-point, or "Triangle," approval process where the Central Technical Authority, SUBSAFE, and the Program Manager must concur before presenting a submarine to the Certification Authority (PEO SUB). See NNBE Report Volumes I and II for additional details.

3. The SUBSAFE Process, presented by the Deputy Director for Submarine Safety and Quality Assurance
   - The Deputy Director placed emphasis in this presentation on the independence of the organization and rigor of development and imposition of the "SUBSAFE Boundaries" that must be managed over the life of a submarine.
   - He also emphasized that no change in the design of the submarine that infringes on these boundaries can be made without first being approved by the SUBSAFE office and subsequently certified for use prior to the ship being released to the Fleet.
   - Finally, the Deputy Director noted that the SUBSAFE organization carries equal weight with the program office in certifying the ship for initial deployment and for subsequent reentry into the Fleet following modifications. Configuration management of these boundaries is sacrosanct.

4. Central Technical Authority in SUBSAFE and the use of Technical "Warrants," presented by the Ship Design Manager for In-Service Submarines
   - The Ship Design Manager presented the concept of a Central Technical Authority and the use of Technical "Warrants" as ultimate technical experts to support the program managers.

- He noted that there are 83 technical warrants at NAVSEA Headquarters and 65 in the field. Selection of warrant holders is through interview with a technical authority board and a one-on-one interview with the NAVSEA Chief Engineer.
- He also explained that warrant authority is conveyed by signatures of Ship Design Integration and Engineering Directorate (Chief Engineer), Commander NAVSEA, and the warrant holder himself.
- Finally, the Ship Design Manager noted that in the event of disagreement between the Program Manager and the Warrant, the PM has the right of appeal to the Chief Engineer.

5. <u>NAVSEA 08's Naval Reactor Safety Assurance, presented by the Director of Reactor Safety and Analysis</u>
   - The Director presented the elements of NAVSEA 08's Naval Reactor Safety Assurance which are also contained in detail in the NNBE Volume II Progress Report of July 15, 2003.

2.7 Pearl Harbor Naval Shipyard & Intermediate Maintenance Facility Audit

NASA personnel observed a NAVSEA SUBSAFE and Deep Submergence Systems (DSS) Functional Audit at the Pearl Harbor Naval Shipyard and Intermediate Maintenance Facility (PHNSY&IMF) conducted February 2-6, 2004. The SUBSAFE/DSS Functional Audit was held concurrently with two other audits: 1) NAVSEA Nondestructive Testing (NDT) Program Evaluation and 2) NAVSEA PMS435 Intermediate-Level Periscope Repair Facility Qualification Audit.

SUBSAFE/DSS audits cover six Functional Audit (FA) areas: Management, Material Control, Quality Assurance, Re-Entry Control, Technical, and In-Process Audit (IPA). The IPA is divided into five distinct sections: Valve/Component Repair/Restoration, Mechanical Joint Make-Up, Welding (Piping and Structural), Testing (Shop/Shipboard), and Non-Destructive Testing. Each FA area was observed by a NASA NNBE team member.

There are two main purposes to the SUBSAFE/DSS Functional Audit. The primary purpose is "to assess the internal processes, procedures, and controls exercised in the performance of SUBSAFE and DSS work to ensure that the activity remains qualified to accomplish such work." In other words, the audit first verifies the adequacy of the existing process and then verifies adherence to the existing process. The audit serves "to provide all levels of management at the activity with an independent, objective, and constructive evaluation of the effectiveness and efficiency with which quality assurance and control responsibilities supporting the SUBSAFE and DSS Programs are being implemented and followed." The SUBSAFE/DSS Functional Audit of an activity is conducted once every two years and is supplemented by an interim audit in the off-year if no SUBSAFE Certification Audit has been conducted during the two-year period. A Certification Audit is performed on an individual ship basis to provide assurance that the material condition of that submarine for systems and components within the SUBSAFE boundary is satisfactory for unrestricted operations to test depth. It differs from a Functional Audit in that functional audits are designed to review processes, controls, procedures, and associated functions used to perform specific SUBSAFE related tasks. In most cases, they are not oriented to a specific ship but are intended to determine how the factors being audited impact SUBSAFE work and the resultant condition for any material or equipment.

Audit Logistics

The NASA NNBE participants attended a pre-audit preparation meeting, in which auditors and observers reviewed audit preparation handbooks. The team held an audit inbrief to provide the Shipyard and the auditors with guidance and set the tone for the audit process. When the audit was completed a few days later, an official outbrief was conducted for the auditors, shipyard Commander, and shipyard personnel. At this outbrief, a senior NAVSEA representative (SES Level) and the audit team leader briefed the shipyard on the overall findings, paying particular attention to the more significant issues identified within each functional area.

Upon return to Washington, the NAVSEA members held an audit debrief at the Washington Navy Yard to review and verify the audit cards, checking for organization, accuracy, and wording. The final version of the audit report was created and presented to PHNSY&IMF at the end of the following week (February 9th – 13th).

To ensure the quality of the SUBSAFE/DSS program, Functional Audits are designed to identify areas where internal processes, procedures, and controls and adherence to those processes could be improved. Table 2 describes the three categories of findings applicable to these Functional Audits.

Table 2. SUBSAFE/DSS Functional Audit Findings

Categories of Findings		
Severity	**Name**	**Description**
High	Certification Finding (CERT)	A Noncompliance finding which could potentially affect the certification status of present and future submarine availabilities. These findings are primarily ship-specific or hardware-related
Medium	Noncompliance (NC)	Violation of local or NAVSEA instructions, procedures, or specifications and/or contracts
Low	Operational Improvement (OI)	Not a specific requirement violation, but may cause degradation in the effectiveness of the SUBSAFE Program or could offer significant improvements in the effectiveness of the SUBSAFE Program

The Functional Audit findings require a response by the appropriate activity, according to the severity of the finding. A Certification Finding, the most severe category, requires a written response submitted to NAVSEA 07Q within 14 days of the audit, and must be approved before the affected ship(s) are allowed to return to sea. Noncompliance and Operational Improvement findings require a written response within 45 days of the audit, and every 90 days thereafter, until the response is accepted by NAVSEA. Responses are evaluated according to standardized criteria contained in NAVSEAINST 4855.35, the "NAVSEA SUBMARINE SAFETY (SUBSAFE) FUNCTIONAL AUDIT PROGRAM."

Potential Opportunities

As a result of the NASA NNBE Team’s participation in the NAVSEA audits held at PHNSY&IMF, several areas where NASA could potentially benefit from NAVSEA best practices were identified. These areas are listed as opportunities below.

Opportunity #1: Establish Clear Audit Boundaries and Verifiable Requirements

For its Functional and Certification audits, the SUBSAFE Program places a high priority on defining clear, measurable, and verifiable requirements. This is absolutely essential to verify compliance. NASA may want to consider an effort to refine its requirements along the same lines, ensuring that each requirement can be accurately assessed and that Objective Quality Evidence (OQE) can be identified and provided to prove compliance.

Along with clear requirements, the SUBSAFE Program establishes distinct boundaries for its audits, ensuring that a defined set of tasks receive focus for a particular audit. Defining the audit's scope prior to audit activity will add emphasis and clarity to SMA audits and will help ensure that the best resources are used to conduct the audit. Clear delineation of Programmatic versus Institutional content being audited will also help structure the auditing process.

Opportunity #2: Provide SMA Requirements Implementation Guidance and Technical Assistance

NASA could potentially benefit from providing requirements implementation guidance and technical assistance to NASA programs and projects, both before and after conducting functional audits. The SMA audit process becomes much more valuable if both the auditors and the audited organization have a clear understanding of requirements. The SUBSAFE Program regularly provides safety and quality assurance requirements implementation guidance and technical assistance visits to programs and institutions in order to ensure requirements are well understood. Requirements implementation guidance and technical assistance from Headquarters OSMA could greatly improve compliance and would foster a much more meaningful auditing process.

Opportunity #3: Create Audit Teams with Individuals from Multiple Organizations and Diverse Backgrounds

NASA could potentially benefit from diversifying its audit teams with highly skilled engineers and technical personnel from across the Agency. Auditing at the PHNSY&IMF was performed by experts from across the NAVSEA organization. A similar approach for NASA, including participants from Center Engineering Directorates, Technical Directorates, Center SMA, Headquarters SMA, Headquarters Enterprises, and other government organizations including NAVSEA, will foster healthy discussion of SMA best practices and help ensure a successful audit process.

Opportunity #4: Coordinate SMA Audits with other NASA Headquarters Review and Assessment Activities

NASA could potentially benefit from conducting coordinated audits with multiple audit teams to reduce disruption of the program/project being audited. During the SUBSAFE/DSS Functional Audit, two concurrent audits were conducted at PHNSY&IMF. This enabled teaming on certain subject areas, where members of one auditing group were able to assist with another. This approach would further be streamlined by acknowledging reciprocity of certification by other audit teams with similar audit requirements.

This page intentionally blank.

3.0 Software Subgroup Report I

This Software Subgroup Report presents an initial report of NNBE findings for software safety and mission assurance, highlighting observations and opportunities derived from two sets of meetings. The first set occurred at the NASA Independent Verification and Validation (IV&V) Facility in Fairmont, West Virginia, July 28 through August 1, 2003, and the second set took place October 6 through 9, 2003, at the Kennedy and Johnson Space Centers.

At the first set of meetings, the Navy attended the IV&V and Office of Safety and Mission Assurance review of software assurance research. The Navy also participated in 1) a presentation on a review of the National Space Development Agency (NASDA) of Japan’s IV&V processes, 2) the NASA/NASDA exchange that followed, and 3) a set of Software Assurance Working Group (SAWG) meetings, in which the new Software Assurance and Safety Standards were discussed.

During the second set of meetings at the Johnson and Kennedy Space Centers, the Navy presented NASA with its software safety and assurance processes for the VIRGINIA Class submarine Ship Control System. Concurrent with these discussions, the Navy reviewed observations and recommendations from a survey of select aviation organizations and programs which develop, field, and maintain fly-by-wire control systems. Since these NNBE discussions, the Navy has adopted a number of these recommendations and codified them in NAVSEA T9044-AD-MAN-010 “Requirements Manual for Submarine Fly-by-Wire Ship Control Systems,” dated April 14, 2004. NASA, in turn, provided the Navy with a look at software engineering, software management, and software safety and mission assurance for the Shuttle program, including launch, flight, test, and payload software.

At these exchanges, both NASA and the Navy identified and described their respective software program management and organizational structures, safety requirements, implementation processes, and compliance verification and certification procedures. By design, these topic areas correspond to the overall framework and structure established at the outset of the NNBE activity. The observations and opportunities identified in this report are also built on and closely tied to the corresponding sections of the previous two reports.

Throughout this section, references to Navy or NAVSEA software development practices refer to the portion of NAVSEA that develops submarine ship control systems. This report does not address processes used for software in other submarine systems, such as Command, Control, Communications, and Intelligence (C3I) or those used in the nuclear reactor plant. As noted in the report, NASA has interest in expanding the review to include submarine systems beyond ship control.

3.1 NASA Software Development & Safety - Summaries and Key Observations

Software Quality Assurance and Safety for NASA's Space Shuttle Program has been examined using the following framework:

3.1.1 Organization
3.1.2 Software Safety Requirements
3.1.3 Implementation Processes
3.1.4 Compliance Verification Processes
3.1.5 Certification Processes

Each section includes a narrative summary and key observations.

3.1.1 Organization (NASA)

Organizational Structure (NASA)

At its highest level, NASA is split into programmatic and functional offices. NASA Enterprises are programmatically focused and are responsible for carrying out the Agency's missions. The functional offices provide supporting roles for NASA, which stretch across all Enterprises. The software NNBE meetings detailed in this report concentrate on the intersection of one programmatic and one functional office: the Space Shuttle Program and the Office of Safety and Mission Assurance (OSMA).

Each NASA Enterprise can be composed of multiple programs, and each program can consist of several projects. The Space Shuttle Program, for example, consists of multiple projects and project managers, located at multiple NASA Centers. The overall Program Manager, along with the Governing Program Management Council (GPMC), may reside at Headquarters or at an individual NASA Center, depending on the program.

NASA functional offices are divided into Headquarters and Center level management. The OSMA organization at NASA Headquarters oversees Agency policies and procedures for Safety and Mission Assurance (SMA) functions, such as health and safety monitoring, mishap reporting, reliability, maintainability, quality, systems safety, probabilistic risk assessment, and software assurance. At the Center level, SMA organizations assign personnel to work with Enterprise projects in areas of project quality, safety, reliability and maintainability. The Center SMA organizations also ensure an independent reporting path for elevating unresolved safety issues to Enterprise project managers, the Center, GPMC, and Headquarters OSMA.

Software plays a critical role in many of NASA's most complex and high profile systems, including the Space Shuttle and International Space Station (ISS) programs. Because the Agency relies on software to complete these missions and ensure human safety, NASA has developed a hierarchical approach to ensure all software is of the highest quality and is as safe and reliable as possible. Both programmatic and functional offices participate in the software and safety assurance processes.

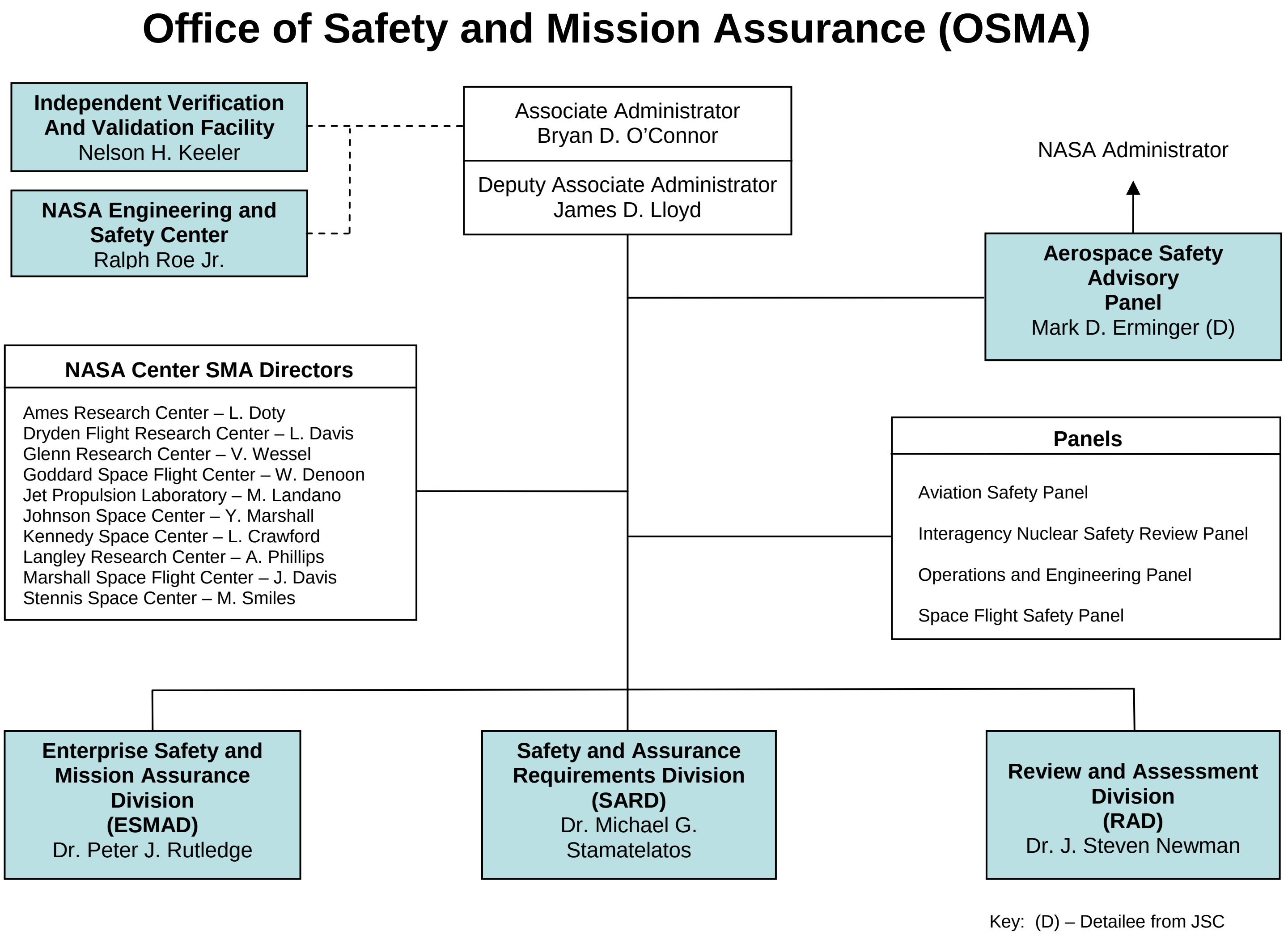
Functional Organization

At NASA headquarters, the OSMA is the functional office responsible for creating, maintaining, and overseeing safety, reliability, maintainability, and quality assurance policies, requirements, procedures, and tools throughout the Agency. OSMA is separated into four main divisions: an administrative division, the Enterprise Safety and Mission Assurance Division (ESMAD), the Safety Assurance Requirements Division (SARD), and the Review and Assessment Division (RAD). ESMAD works with the SMA organizations at each NASA center, ensuring that OSMA has insight into every program within the Agency. This division is also the liaison to Enterprises at NASA, which are charged with fulfilling the Agency's missions. SARD focuses on the disciplines of Safety, Reliability, Quality, and Assurance, and manages the policies, standards, and tools which relate to these disciplines. The recently-formed RAD performs audits and independent assessments for OSMA, and provides ongoing benchmarking with private industry and other government organizations. OSMA also manages the NASA IV&V Facility and has recently joined with the Chief Engineer's office to oversee the NASA Engineering and Safety Center (NESC). The OSMA organization is represented in Figure 5.

Software Assurance represents only one aspect of SMA, but it is addressed across all the divisions of OSMA. The OSMA administration oversees the IV&V Program, which performs independent analysis and verification procedures for selected safety and mission critical software programs. ESMAD coordinates with the Center SMA organizations, helping them fulfill NASA's policies and procedures, including those for software assurance. Software assurance and safety standards and policies are created and maintained by SARD, which also provides funding and oversight for software assurance training and research throughout the Agency. Lastly, RAD conducts software-related audits for NASA programs and performs independent software assessments either standalone or as part of a larger effort. The NASA/Navy Benchmarking Exchange is one such assessment. Each of the four OSMA divisions plays a role in assessing the performance of software assurance across the Agency. Together, they comprise NASA's overarching approach to SMA for software.

Software Assurance

NASA's Software Assurance (SA) efforts are divided into Headquarters and Center organizations. Center SA representatives work on day-to-day issues with the projects at their NASA Center. Their primary focus is to assure software processes are in place and carried out effectively, and that software products meet all their requirements, especially those for safety and quality. SA is conducted throughout every phase of the software life cycle. At NASA Headquarters, SA concentrates more on Agency-wide issues, such as research into new software assurance and safety procedures, developing and updating standards, establishing and maintaining policies, and participating in reviews and assessments of both software and software assurance functions within the Agency.



Office of Safety and Mission Assurance (OSMA)

Independent Verification And Validation Facility
Nelson H. Keeler

NASA Engineering and Safety Center
Ralph Roe Jr.

Associate Administrator
Bryan D. O'Connor

Deputy Associate Administrator
James D. Lloyd

NASA Administrator

Aerospace Safety Advisory Panel
Mark D. Erminger (D)

NASA Center SMA Directors

Ames Research Center – L. Doty
Dryden Flight Research Center – L. Davis
Glenn Research Center – V. Wessel
Goddard Space Flight Center – W. Denoon
Jet Propulsion Laboratory – M. Landano
Johnson Space Center – Y. Marshall
Kennedy Space Center – L. Crawford
Langley Research Center – A. Phillips
Marshall Space Flight Center – J. Davis
Stennis Space Center – M. Smiles

Panels

Aviation Safety Panel
Interagency Nuclear Safety Review Panel
Operations and Engineering Panel
Space Flight Safety Panel

Enterprise Safety and Mission Assurance Division (ESMAD)
Dr. Peter J. Rutledge

Safety and Assurance Requirements Division (SARD)
Dr. Michael G. Stamatelatos

Review and Assessment Division (RAD)
Dr. J. Steven Newman

Key: (D) – Detailee from JSC

Figure 5. NASA Organizational Structure.

Despite the differences in job focus and the small number of SA personnel within NASA, Headquarters and Center SA have a very close working relationship. The SA group places a strong focus on active and extensive collaboration. The Headquarters SA Manager has organized a Software Assurance Working Group (SAWG) which holds at least bi-monthly meetings and has a very active and detailed working website. The SAWG helps formulate and write the standards and policies for software assurance and software safety, which they also help to implement on NASA programs. The working group also engages regularly with the NASA Software Working Group managed by the Chief Engineer's Office, another functional office within NASA. The Headquarters SA Manager and the Software lead in the Chief Engineer's office work on a daily basis to assure a consistent Agency-wide approach to NASA's software policies, procedures, initiatives, and programs.

SA personnel from the SMA organizations participate in formal and informal reviews on NASA projects, sit on software control boards, and perform audits on software products and processes. SA is integral in performing the Functional and Physical Configuration Audits, which are used to verify that the software products and processes are complete and ready for system integration or operation.

Programmatic Organization

Based on the Center SMA assessment and recommendations, each project develops a specific approach to implementing an agreed-upon set of SA tasks. The program/project determines the software-specific project requirements, including technical system requirements, coding standards, language, methodology, system architecture, and the "make or buy" decision for software. Center and/or contract SA may provide input to these decisions; however, they are the project manager or project software manager's responsibility.

The first task of the independent Center SA organization is to assess the software risk of a project. From this assessment, the SA organization recommends to the project a set of tasks, analyses, and procedures for mitigating software risk on the project. For new projects, this assessment must be created from the ground up. For maintenance or changes to software, an original assessment should already exist, and SA monitors changes that will impact or alter the original assessment.

From the SA assessment, the project manager and Center SA establish a written agreement as to what tasks will be performed and by what organizations. Center SA, the program engineers, or contractors may perform the tasks, analyses, and procedures required for all disciplines of SA, with the exception of IV&V. When independent verification and validation is designated for a project, it must be performed by NASA's IV&V Facility. However, it remains the responsibility of the Center SMA organization to make sure that the project has actually performed all tasks, analyses, and procedures identified in the SA assessment, and to notify the program manager of any deviations from this assessment.

Independent Verification and Validation

The NASA IV&V Facility was established in 1993 to "provide the highest levels of safety and cost-effectiveness for mission critical software." The IV&V Facility is headquartered in Fairmont, West Virginia, though many IV&V agents work onsite with project development teams. OSMA oversees the IV&V Program, and while IV&V is a separate and independent facility, functionally it is considered a discipline within SA. The day-to-day operations of IV&V are controlled by the IV&V Facility Director, who doubles as the Program Manager for IV&V. The program is tasked with independently monitoring certain safety and mission critical projects throughout their life cycle, commensurate with each project's level of criticality and risk. IV&V employs approximately 150 people, the majority of whom are contractors, and it performs independent assessment activities including product verification, analysis, and some limited testing. IV&V follows industry best practices, and is technically, managerially, and financially independent from the software projects to which it is assigned.

Key Observations: Organizational Structure

- NASA's organization is divided into programmatic and functional offices. Both participate in SMA processes and policies.
- The OSMA is the functional office specifically charged with overseeing SMA for NASA, which includes software. It is divided into Headquarters and Center level organizations. SA is addressed as a function of overall SMA, while IV&V is treated as an independent software SMA organization within the office.
- Each Enterprise within NASA is charged with adopting SMA processes for a particular program or project. Software SMA on a programmatic level is typically governed by control boards and review panels.

Technical Authority (NASA)

Technical authority for all NASA projects has historically resided with program or project managers. Currently, these managers are in charge of selecting all software standards and procedures to be used on their projects, and they must ensure that these standards and procedures are followed. Until recently, program and project managers have been allowed to choose the standards to which they felt their projects should adhere. These could have been NASA, industry, or Department of Defense standards as they chose, or as the contractors preferred. NASA is in the process of changing this policy and is preparing to require that Agency-wide Software Assurance and Software Safety standards be applied to all projects. The use of other standards will be allowed, but each project will be required to meet the minimum requirements of the NASA standards. The manager of software development is also charged with adherence to standards levied by the Center and all program or project specific standards.

NASA is developing and beginning to apply an Agency-wide software categorization scheme that takes into account tasks the software has to perform and the mission risks associated with those tasks. Risks are assessed based on the complexity of the software system, the level of control the software exercises, the level of innovation of the software and its development processes, the organizational complexity, the likelihood of on-time and on-budget completion, and facility, vehicle, personnel, and environmental consequences. While a software safety “litmus” test is used to help determine whether the software will perform any safety critical functions, actual and potential software safety hazards are derived from the system hazard analyses.

For low-risk software implementations (i.e., projects of low cost, low complexity, little innovation, and small impact to a NASA mission), the project manager receives little outside assistance on SA processes and tasks. As risk increases, a higher degree of insight and oversight is applied to a project from contractor and Center SMA offices. For all safety critical software, Center SA and, when deemed necessary, IV&V, are assigned to the project. The SA representatives act as advisors on the program, notifying the manager of any safety or quality concerns as early as possible. With the advent of NASA’s new software assurance policy, implemented in July 2004, SA is tasked with ensuring a project’s adherence to the software safety and assurance standards and will actively participate in any waivers or deviations from the requirements in those standards.

When independent validation and verification is selected for a software project, it is managed through NASA’s IV&V Facility. The IV&V organization has the technical authority to choose which software products of the project will be analyzed, and to what extent.

While both IV&V and SA serve mostly in an advisory role to the project or program manager, Headquarters OSMA is the single authority for final sign-off on safety critical missions. Most decisions on a project, including decisions concerning safety critical software, are made by the project manager. But in practice, the tremendous focus NASA places on safety and mission assurance causes program/project managers to listen very closely to the recommendations of these organizations. It is rare that a recommendation from either SA or IV&V is not implemented on a program.

In the event of serious disagreement between these independent organizations and the program or project manager, a safety concern may be escalated. It happens very rarely, but both SA and IV&V have the capability to appeal an issue all the way to OSMA for arbitration, if they feel a safety concern has not been adequately addressed at the lower levels. This independent reporting structure is designed to ensure that potential hazards can be addressed at the highest level necessary, reducing the chance of a single point of failure for safety critical systems.

Key Observations: Technical Authority

- The project or program managers (PMs) have historically been the technical authority for their individual NASA projects.
- The project or program manager is required to create a software plan for a project that is compliant with NASA’s Software Assurance and Software Safety standards.
- Center SA and IV&V perform advisory roles on projects, in proportion to software criticality. They also serve as an independent reporting authority for safety issues.

- While the PM is ultimately responsible for safety, both SA and IV&V have the capability to appeal an issue all the way to OSMA for arbitration, if they feel a safety concern has not been adequately addressed on a program.

Resource Management / Procurement (NASA)

Once the NASA budget has been approved and goes into effect, funds for each program/project are allocated to the program/project managers. Each project reports its risk management plan, status, budget, and schedule to the Governing Program Management Council (GPMC). The GPMC may exist at the Center under the Center Director, or at Headquarters under the program management office for the respective Enterprise. The Program Management Council is at Headquarters.

Programs usually break down into several projects. Each project divides into functional pieces (such as software), and some are split again across Centers. Shuttle software projects, summarized in Figure 6, are a good illustration of this work allocation.

Johnson Space Center	**Kennedy Space Center**
▪ Shuttle Flight Software – Primary Avionics Software System (PASS) – Backup Flight System (BFS) – Cockpit Avionics Upgrade (CAU) ▪ Shuttle Avionics Integration Laboratory ▪ Flight Control Room Software	▪ Launch Processing System (LPS) ▪ Checkout and Launch Control System (CLCS) – Only implemented at Hypergolic Maintenance Facility (HMF) ▪ PCGoal and PCGoal2 ▪ Orbiter Checkout and Test Facilities ▪ Kennedy Avionics Test Set (KATS)
Marshall Space Flight Center	**Stennis Space Center**
▪ Space Shuttle Main Engine Control (SSMEC) software	▪ Main Engine and Reaction Control Systems Testing

Figure 6. Shuttle Software Projects.

Once a project receives funding and the contracts are established, the project manager works with the procurement offices to oversee and manage contract deliverables. Each NASA Center has a procurement office that is charged with product and service acquisition for projects at the Center. For large programs, NASA typically delegates actual development tasks to a prime contractor, selected through a competitive bidding process. Often, a prime contractor will in turn contract out products and services outside its area of expertise to a subcontractor.

Over the past ten years NASA has applied a form of performance-based contracting to many new projects and programs, including software implementations. Under the strictest definition of performance-based contracting, an organization gives a contractor a set of detailed requirements, and asks the contractor to design, develop, and test a system based on those requirements. The system is then verified by the organization during its development and after the final product has been completed.

Industry trade studies have found that performance-based contracting is most successful when requirements are very well documented and clearly understood by all parties. Like all R&D activities, requirements definition can be difficult on many of NASA's projects because the Agency is performing tasks that have never been done before. As a result, the final specifications NASA sends to its contractors may not be well-defined, representing goals more than true requirements. Under these circumstances, contractors may not be able to interpret the requirements correctly, and, when the finished product is delivered to NASA, it may require redesign.

As the number of NASA civil servant engineers has decreased, contractors have played more important roles in the development of NASA's systems. NASA engineers and developers work closely with contractors, exploring design options and requirements restrictions as the project develops. The link between civil servant and contractor is essential for NASA to manage its projects and programs, and it also serves to minimize the cost of requirements definition for future projects. Software assurance of safety critical systems is a joint effort between civil servant and contractor, and the Agency depends on contractors to perform software assurance in accordance with NASA or their own standards.

After a development project or program becomes operational, NASA takes a more active management role. However, the Agency continues to use contractors for the day-to-day maintenance and upgrades to the system. In the maintenance phase of a software project life cycle, NASA has developed a highly integrated approach to contractor management, where civil servants work in the same physical location as contractors, often sharing tasks and corroborating on software development. This integrated method attempts to create a non-adversarial relationship between NASA and its contractor and causes overall software requirements goals to become more closely aligned. NASA's project development teams, with highly integrated mixtures of NASA and United Space Alliance (USA), a Boeing, Lockheed-Martin joint-venture, personnel all working side-by-side, produce a single, integrated software product.

Key Observations: Resource Management / Procurement

- Each project reports its risk management plan, status, budget, and schedule to the GPMC or the PMC.
- NASA has applied a form of performance-based contracting to many new projects and programs, including software implementations.
- NASA has developed a highly integrated approach to contractor management, where civil servants work in the same physical location as contractors, often sharing tasks and corroborating on software development.
- The link between civil servant and contractor is essential for NASA to manage its projects and programs, and it also serves to minimize the cost of requirements definition for future projects.

3.1.2 Software Safety Requirements (NASA)

Safety Philosophy (NASA)

As with all safety-related systems and processes, NASA has adopted a conservative approach to software safety. Despite processes and analyses, stringent requirements, and rigorous testing, the Agency operates under the assumption that there may be some condition under which a single software program may eventually fail. The current procedures, requirements, and even software architecture stem from over 25 years of experience in Shuttle system software. It is standard policy that no level of inspections, processes, techniques, or testing can guarantee that software will be fully operational and provide correct information in all situations. Therefore, to be truly safe from software-induced hazards, controls for safety critical software must exist outside of a single software program and platform. Controls implemented by the Space Shuttle Program have included multiple redundant hardware systems; backup software systems that are designed, coded, and tested separately from primary systems; and system safety techniques, which include the shutdown and reboot of affected software. In many cases, these external controls have never been used. However, their existence provides further safety assurance and a greatly diminished potential for failure.

A second overarching philosophy comes from years of experience with safety critical systems. NASA places a strong focus on designing and building safety into a system, instead of addressing safety issues after software or hardware development is completed. Software safety issues are prominent in all phases of the development life cycle, beginning with system requirements. This “front-loading” of safety concerns into a software system accomplishes two important tasks. First, software changes can be more easily assessed for their potential impact on system safety in the initial stages of software development. By catching and fixing safety issues early, a project is able to save time and money necessary for later insertion (which may impact designs and increase testing) and also assure that the safety design is integrated into the system and software in a cleaner manner. In addition, by emphasizing safety early in the software life cycle, developers are allowed more intensive scrutiny of possible system hazards and are thus able to find better ways to mitigate, control, and eliminate potential hazards. Ultimately, this results in safer, more straight-forward software.

For existing safety-critical software, NASA has adhered to a philosophy of embedding software safety into a system through clear safety requirements and established safety processes. The Agency believes that defects within its software can almost always be traced to missing or misunderstood requirements. Inadequate safety processes and skipped safety checks have often been contributors to these defects as well. Very few problems with the software design and implementation have led to failures. Root cause analysis of unexpected defects usually result in process changes. As project management comes to a better understanding of software and software safety, the safety processes and procedures for change control will be better followed and modified as needed.

Key Observations: Safety Philosophy

- NASA assumes that software can always fail, despite best efforts to ensure safety, reliability, quality, and maintainability.
- True software safety requires building safety into the system throughout the development life cycle, rather than adding safety as an afterthought.
- While software deficiencies are addressed as they are discovered, unmitigated hazards are traced back to their root causes and considered a result of flawed requirements or a flawed safety process. NASA believes safe, high-quality software is a byproduct of continually updated, refined, and validated software SMA processes. By fixing processes rather than just problem occurrences, future problem occurrences are reduced.

Governing Documents (NASA)

NASA Policy Directives (NPDs) and NASA Procedural Requirements (NPRs) are the primary documents used to define high-level processes, requirements, roles, and responsibilities for the Agency. NASA defines Safety Criticality from the definition of Hazard Severity in Chapter 3 (System Safety) of NPG 8715.3, the NASA Safety Manual, and additional supporting information is located in Appendix-D (Analysis Techniques) of the same document. NASA's standards address *what* needs to be done, and they are aimed more at the practitioner and project management level. A set of guidebooks provide information on *how* it should be done, including checklists, examples, and scenarios for the practitioner.

NASA's overarching Software Assurance Standard, signed on July 28, 2004, and Software Safety Standard, signed on July 8, 2004, define a process-based approach to assuring software safety, quality, reliability, and maintainability through all phases of the software life cycle, from conception software assessments and request for proposal (RFP) considerations, through requirements gathering and development, to program completion. In most cases, these documents closely follow industry standard processes and comply with standards from the Institute of Electrical and Electronic Engineers (IEEE); however, both are specifically tailored to NASA and how NASA conducts business. For instance, these documents show the balance of SA's disciplines of safety, reliability, V&V, IV&V, and quality engineering.

These documents are extremely broad in their approach, defining what must be done to assure software quality and software safety, but not how it must be done. While there are NASA guidebooks for software safety (including one that is being updated for software assurance), how these functions are carried out is at the discretion of the program manager, or found in center-specific and program-specific standards or processes. These guidebooks and Center or program procedures are often more technical and more detailed, and serve both to complement the Agency-wide standards and to tailor quality and safety assurance to individual projects. This "layered" approach to documentation standards allows NASA to customize SA to a level appropriate for each project, and allows differing standards for design/build and maintenance/ upgrade projects.

<u>Key Observations: Governing Documents</u>

- The Software Safety Standard and Software Assurance Standard are the overarching requirements documents for software SMA. In most cases, these documents closely follow industry standard processes and comply with IEEE standards; however, both are specifically tailored to NASA.
- While there are NASA guidebooks for software safety, how these functions are carried out is at the discretion of the program manager or found in Center-specific and program-specific standards or processes.

Requirements Flow Down / Ownership (NASA)

While the Software Assurance Standard and Software Safety Standard written by OSMA are designed to be comprehensive, they are also designed to be general, covering and applying to all NASA software projects. Centers and programs are left to apply the Agency-wide requirements to their projects and, in order to better reflect the operational environments and technical details of the software for their systems, develop additional requirements of their own,. The Space Shuttle Program, for example, has developed its own set of standards that are particular to the unique characteristics and needs of the Space Shuttle and the environment in which it operates. All members of the Space Shuttle software development teams must follow these standards, including civil servants and contractors.

It is the responsibility of a program or project manager to assign safety requirements for software, but all requirements must comply with overarching NASA requirements and all relevant Center or Program requirements that exist. Using these as a baseline, the program manager is able to establish additional, project-specific standards and policies. NASA program or project managers therefore have historically owned all software standards and procedures to be used on their projects, and they must assure that these standards and procedures are followed. The multiple levels of safety requirements allow a great deal of flexibility for each software implementation and result in different approaches to software safety implementation and processes across programs within NASA while maintaining a consistent awareness and respect for the safety process.

Program variations, however, have led to instances where the software assurance and safety standards have not been followed as closely as expected. In coordination with the release of the revised NASA software standards, Center SA personnel will more aggressively track each project's adherence to these standards. As mentioned previously, both SA and IV&V are relegated to advisory roles within safety-critical programs. It is only when these organizations believe a software project has the potential to create a hazard, and that the hazard has not been fully addressed, that the program manager may be overruled on requirements for a particular project. In these rare cases, the issue is elevated through the OSMA independent chain.

Key Observations: Requirements Flow Down / Ownership

- The project or program manager has historically owned project-specific SW requirements. Software Assurance personnel track a project’s requirements and their adherence to the overarching Software Assurance Standard and Software Safety Standard.
- Specific software SMA requirements are often created at the program or project level, but all such requirements must be compliant with the governing Software Safety Standard and Software Assurance Standard.

3.1.3 Implementation Processes (NASA)

Software Safety Implementation (NASA)

Not all Program software is considered safety-critical. Before a project is assigned to comply with safety-critical standards, it must first be identified as a project that requires those criteria. In its revised Software Safety Standard, NASA identifies safety critical software by first assessing the hazard severity for the software project and then by assessing the functions of the software itself, including its potential to contribute to an identified hazardous state.

Figure 7 describes the four system levels of hazard severity used by NASA to identify safety critical software. If the software has a potential to contribute to a catastrophic or critical hazard, it is automatically classified as safety critical software and is subject to additional levels of inspection, testing, and certification as detailed by the NASA Software Safety Standard. The Agency has further defined how software may contribute to a potential safety hazard. The *Software Safety "Litmus" Test* presents project managers with a set of criteria to define safety critical software. If any of the five criteria apply to the software, it is automatically deemed safety critical. An example of the Software Safety Litmus Test is represented in Figure 8.

Hazard Severity Definitions	**Catastrophic** - Loss of human life or permanent disability - Loss of entire system - Loss of ground facility - Severe environmental damage	**Critical** - Severe injury or temporary disability - Major system or environmental damage
	Moderate - Minor injury - Minor system damage	**Negligible** - No injury or minor injury - Some system stress, but no system damage

Figure 7. Hazard Severity Definitions.

Once a project is identified as safety critical, the entire project life cycle is planned to assure compliance with safety critical processes. Starting with the System Preliminary Hazard analyses to determine the system's hazards, software's role in contributing to or mitigating these hazards must be explored. SA personnel are charged with reviewing and either implementing or assuring implementation of a software safety plan, which defines the processes and analyses for identifying and tracking all potential hazards in the system, as well as mitigation and control strategies. Ultimately, one or more SA discipline representatives are charged with certifying a software system as safe for its intended use. All results are then reported to the project or program manager.

Software Safety Litmus Test			
Does the software do any of the following?		**Yes**	**No**
1.	Control or monitor any safety critical functions?		☑
2.	Act in part, or in whole, as a control or mitigation to a hazard?	☑	
3.	Act as the test, simulator, or model for safety critical software or hardware?		☑
4.	Run on the same processor as safety critical hardware?		☑
5.	Detect and report either faults or trends that indicate a potential hazard, or failures which lead to a hazardous condition?		☑
If any boxes are marked "Yes," the software is **Safety Critical**			

Figure 8. Software Safety Litmus Test Example.

Key Observations: Software Safety Implementation

- Software SMA Requirements depend on the nature of the project. In NASA's revised Software Safety Standard, all projects will undergo a hazard severity and safety analysis in order to determine the appropriate level of software SMA applied throughout the life cycle of the project.
- SW Safety "litmus" test criteria are used to identify safety critical software.

Software Safety Approach / Analysis Tools (NASA)

All NASA systems begin with a Preliminary Hazard Analysis (PHA), which is developed during the initial requirements phases. The PHA identifies potential safety hazards for the system and is the beginning of all safety decisions on a project. The PHA is updated and changed as requirements and design choices are made throughout the software life cycle, and these hazards and impacts to these hazards are constantly examined throughout the development process. Additional safety and reliability analyses continue as the system development matures. A system hazard report is written and updated, including explanations of how specific safety controls and mitigations will reduce or control potential hazards. It also addresses the verification procedures for ensuring all safety requirements, controls, and system staffing functions will work.

In past NASA projects, software participation in safety analysis processes had been late or lacking. Until recently, Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA), which are regularly performed on hardware, were considered too difficult or unnecessary for software systems. However, as newer projects have been implemented, software safety has been considered at earlier points in the development life cycle – from design requirements, to testing for safety impacts, to coding error detection and responses.

Based on the *Software Safety Litmus Test*, the designation of a new project as safety-critical during the concept development phase will allow SA to play a greater role in the entire life cycle of the project, ensuring each step is correctly considering software safety. In addition, identifying and tracking potential software contributions to identified system hazards during concept development will help ensure future safety-critical requirements are as comprehensive as possible.

For NASA's software maintenance and upgrade projects, a fully developed and functioning software system exists with all safety critical system aspects identified and tracked. These projects are typically the result of new features, COTS software upgrades, or bug fixes. In fact, a number of maintenance issues arise because of software safety risks inherent in an existing system. Examples of existing software currently undergoing maintenance and upgrades in the Space Shuttle Program include the Launch Processing System and PCGOAL at Kennedy Space Center, and the Shuttle Flight Software at Johnson Space Center.   *Note: The PCGOAL System (Personal Computer Ground Operations Aerospace Language) is a legacy name which describes a group of computers used to maintain the Shuttle Data Stream during flight. The platform is not actually built on the GOAL language.*

Upgrading COTS software, especially safety-critical software, is often very expensive, as extensive testing must be done to ensure the new version of software will not present a hazardous condition for the crew. NASA has attempted to minimize software upgrades to its systems for this reason, preferring to use established software versions for as long as possible. Indeed, many safety-critical software systems, from shuttle flight software to launch control software, are as old as the Shuttles themselves. While the Agency frequently updates its own software, it has seldom made use of scheduled upgrades for COTS Software.

NASA adheres to a philosophy of embedding software safety into existing system. In the case of bug fixes, NASA tracks software deficiency reports and performs formal causal analysis to determine the root cause of the defect. In NASA's experience, very few problems with software design and implementation have led to failures. More often than not, formal causal analysis has determined that missing or misunderstood software safety requirements, inadequate safety processes, or skipped safety checks have been the root cause of the defect. This usually results in safety process and procedure changes that are incorporated into existing systems through improved project management understanding of software safety requirements.

Key Observations: Software Safety Approach / Analysis Tools

- Software safety has been considered at earlier points in the tool development life cycle, thus allowing earlier proactive reduction of safety errors.
- Based on the *Software Safety Litmus Test*, the designation of a new software project as safety-critical during the concept development phase will help ensure software safety is considered correctly in each step of the project life cycle.
- NASA rarely makes use of scheduled upgrades for maintenance and upgrades of COTS software because it can be very expensive and require extensive testing.

Instead, NASA has tried to minimize by using older and more established versions of its own software for as long as possible.

- NASA tracks software deficiency reports and performs formal causal analysis to determine the root cause of software defects.

Software Quality Implementation (NASA)

NASA is employing common frameworks for software process improvement. The Agency recognizes the Software Engineering Institute (SEI) Software Capability Maturity Model® (CMM®)[2] and CMM-Integrated (CMMI®) processes as proven frameworks for advancing software engineering practices and as key elements in achieving some of NASA's goals. Shuttle Flight Software has a long history of being an early adopter of CMM, and it was one of the first organizations nationally to be assessed at CMM level 5 (the highest level) in the early 1990s. Since that time, NASA's contracting organizations for Shuttle flight software have changed twice (from IBM FSD to Loral to USA), but the rigorous procedures and processes have been adopted across contractors. Although NASA has set the bar high in the use of CMM early within the Shuttle Program, it has taken substantial time for its adoption in practice by lower profile projects. NASA instituted an Agency-wide software improvement initiative (the Software Engineering Initiative, led by the Office of Chief Engineer) in 2001 that relies heavily on CMM/CMMI.

Key Observations: Software Quality Implementation

- NASA has accepted the Software Engineering Institute Software Capability Maturity Model and CMM-Integrated processes as key elements in achieving some of NASA's goals.
- Despite changes in NASA's contracting organizations for Shuttle flight software, the rigorous procedures and processes have been adopted across contractors.
- An Agency-wide software improvement initiative, begun in 2001, relies heavily on CMM/CMMI.

Training (NASA)

The Space Shuttle Program has an extensive training regimen across all of its systems, including software. The process combines training classes, simulations, and certifications to ensure personnel are completely capable of performing the tasks required. A strong emphasis is placed on mentoring and on-the-job training because the systems are so unique and require so much attention to detail that it is impossible to grasp the entire system in a class environment. For many of the systems, NASA employees are trained for several years before they are able to

[2] *The Capability Maturity Model: Guidelines for Improving the Software Process*, Software Engineering Institute at Carnegie Mellon University, Addison-Wesley (1994), ISBN 0-201-54664-7. Capability Maturity Model and CMM are registered (®) in the U.S. Patent and Trademark Office. Reference, herein, to any specific commercial product, process, or service by trade name, trademark, or otherwise, does not constitute or imply its endorsement by the United States Government.

complete their assigned tasks without the supervision of mentors or senior personnel. The extensive training required, coupled with the decades since much of the software was designed, has resulted in a shortage of personnel that truly understand Space Shuttle Program software.

<u>Key Observations: Training</u>

- The Space Shuttle Program has an extensive training regimen for software systems that includes classes, simulations, and certification of qualified employees.
- NASA places a strong emphasis on mentoring and on-the-job-training as part of its training program due to the uniqueness and complexity of its systems and associated software.

Life Cycle Extension / Modernization (NASA)

The Space Shuttle program has operated beyond its original operational timeframe. The fact that the program has been extended much longer than originally designed has resulted in a number of difficult issues for program engineers to solve. The Shuttle Life Extension Program (SLEP) is currently being addressed by a NASA-wide team dedicated to studying and understanding the ramifications of using the 25-year-old shuttles until their retirement in 2010. While the team is currently focusing on hardware aspects of Shuttle life extension, the Shuttle software program manager and his team are addressing every software aspect required to keep the Shuttle running.

Although much of the Space Shuttle Program’s software is currently in the maintenance and operations phase of the software life cycle, participants to the NNBE meetings were able to see two current Shuttle software modernization projects – the Cockpit Avionics Upgrade (CAU), which will update the cockpit displays for the Space Shuttle, and the Checkout and Launch Control System (CLCS), which was designed to replace the Launch Processing System Software at Kennedy Space Center.

The CAU represents a typical example of Shuttle avionics modernization. The Shuttle crew requested better means to see and interface with the Shuttle flight systems. The CAU represents a significant modernization of Shuttle flight software and is actually classified as a separate project under the Shuttle program. It will continue to be run as a separate project until its final integration into the current Shuttle systems. When completed, the CAU will result in a new user interface for astronauts on board the Shuttle, allowing easier access to information and providing enhanced safety features to the crew. A different program manager oversees this effort and closely coordinates with the Shuttle managers to ensure each incremental upgrade is thoroughly understood, verified, and validated. The CAU was assigned a separate set of safety and SA personnel to perform software safety and assurance for the project.

All requirements for the CAU were extensively reviewed by the Shuttle flight software and systems experts, the crew, Mission Operations, and Center SMA from both the contractor and NASA sides of the program. Once the requirements, general layout, and look of the screens were determined, NASA designed for incremental upgrades, one Shuttle at a time, until the full set of requirements had been met, tested, and integrated. The use of the Shuttle Avionics Integration Laboratory (SAIL), which functions as NASA's fourth Shuttle for the purposes of software testing, is crucial in testing all changes to the Shuttle software and crew interfaces.

CLCS was an attempt at a complete system redesign and upgrade for the Launch Processing System. The computer platforms, language, architecture, and interfaces were all redesigned as a part of this effort. Software Assurance played a critical role in monitoring software safety on the project, though its role began late, during the design phase of the project. Like the CAU implementation, the CLCS project was run as a phased effort, where only one part of the LPS system at a time was to be replaced. However, during the late stages of development, the CLCS project was cancelled due to budget and schedule overruns. Only the Hypergolic Maintenance Facility (HMF) has been able to experience a completed, tested, and installed CLCS system. The HMF application set is currently being maintained for a short period of time, but the facility is scheduled to revert back to the LPS system soon. Although the new HMF software system provides enhanced safety improvements, a better user interface, and increased functionality, the cost of maintaining both the LPS and CLCS software has been judged too costly for the project to continue.

The CLCS project represents an attempt at life cycle extension based on a complete system redesign in the Shuttle program. The inability to implement the new software for the entire system, however, caused users to revert back to the old Launch Processing System (LPS). The new focus of the LPS project is to try to find ways to upgrade in smaller increments, modernizing the system gradually. LPS software designers plan to switch to a higher order coding language from the LPS specific language and replace the nearly 30-year-old computers with modern machines. The goal is to allow the LPS system to escape obsolescence by gaining enough memory and CPU capability to be able to handle needed changes to the Orbiter Processing Facilities (OPFs) and LPS controls.

<u>Key Observations: Life Cycle Extension / Modernization</u>

- For the Space Shuttle, technology insertion / modernization projects are formed separately from the rest of Shuttle flight software and are run as a separate, phased projects up until final integration into the current Shuttle systems.
- All Shuttle technology insertion / modernization requirements are extensively reviewed by the Shuttle flight software and systems experts, the crew, Mission Operations, and Center SMA from both the contractor and NASA sides of the program.
- The use of the Shuttle Avionics Integration Laboratory (SAIL), which functions as NASA's fourth Shuttle for the purposes of software testing, is crucial in testing all changes to the Shuttle software and crew interfaces.

3.1.4 Compliance Verification Processes (NASA)

Quality Reviews (NASA)

For the Shuttle, design verification is achieved primarily through peer reviews and formal reviews. Both contractors and NASA civil servants are closely involved in the process. Design changes are first approved by change control boards, and then implementation is verified through peer reviews and testing. Successful results of tests and reviews are returned for evaluation to the change control boards, which then close the action that initiated the change.

For the Launch Processing System (LPS) at Kennedy Space Center, software design is updated with each change to a software set. Software designs are verified by a combination of peer reviews of design documentation, technical reviews, and integrated testing. Technical reviews include the following Technical Review Panels: Design Requirements Review, Preliminary Design Review, Critical Design Review, and Verification Readiness Review. Both NASA civil servants and the primary contractor participate in these reviews. The LPS software is accepted by the end user during the Software Verification test process.

The PCGOAL system is a certified system within the LPS framework that is currently being upgraded. Certification for this system is accomplished by the KSC Design Certification Review process, a process which both civil servants and the primary contractor are responsible for following.

Key Observations: Quality Reviews

- Design verification for the Space Shuttle is achieved primarily through peer reviews and formal reviews from technical experts following structured processes and using consistent and thorough review checklists.
- Change control boards authorize changes and participate in formal reviews. These boards have both NASA and contractor representation, but changes must be approved ultimately by a NASA manager.

Work Review Processes (NASA)

Shuttle flight software has a very strong software inspection process it has maintained for more than two decades. The data generated by Shuttle inspections is very insightful and can be compared to the program's historical data base. Out-of-tolerance indicators from this data can catch problems early, keeping them from propagating into later quality gates (testing, etc.) where their probability of escaping into operations is higher. The Space Shuttle Program points to their software inspection process as a key foundation of their excellent quality record in developing, implementing, and verifying mission critical software.

Key Observations: Work Review Processes

- Shuttle Flight Software has a very strong software inspection process that has been maintained for more than two decades. Out-of-tolerance indicators can catch problems early, keeping them from propagating into later quality gates (testing, etc.) where their probability of escaping into operations is higher.

Audits (NASA)

Functional & Program Compliance Verification Audits will be regularly performed by OSMA for all NASA Center SMA offices and Headquarters offices. The main purpose is to ensure that the Center and Headquarters, where appropriate, know, understand, and carry out NASA's SMA requirements. There is a need to perform more regular audits of contractor and NASA Software Engineering by NASA SMA organizations. Headquarters SA is required to audit Center SA functions yearly to satisfy CMM/CMMI assessments for those attempting to achieve Level 2 and above.

Key Observations: Audits

- There is a need to perform more regular audits of contractor and NASA Software Engineering by NASA SMA organizations.

Control Boards (NASA)

For large programs, software control boards are an important aspect of managing software risks (including budget and schedule risks) and verifying software requirements implementation and compliance. For the Space Shuttle Program, shuttle flight software, launch processing software, and mission control software each have their own hierarchy of software control boards. These boards are project-specific, and report directly to the program manager or to parent control boards. Both NASA civil servants and contractors are generally seated on these boards.

At Johnson Space Center, the Shuttle Avionics Software Control Board (SASCB) governs all proposed changes to Shuttle flight software, as well as interfaces between Shuttle flight software and other Shuttle-related software. Both Shuttle contractors and NASA civil servants sit on the SASCB, but the board is chaired by a NASA civil servant who is required to sign off on all changes. The board meets weekly to discuss flight software changes.

Software change control for the Launch Processing System (LPS) at Kennedy Space Center is governed by the Integrated Data Systems Change Control Board (IDS CCB), which is co-chaired by a NASA civil servant and a contractor. All proposed changes to LPS software must be approved by both co-chairs of the IDS CCB. However, control over the change process does not end here. A number of subsidiary boards, more specific and technical than the IDS CCB, are required to approve changes throughout the software life cycle. Each board is assigned approval authority for a specific software development process: requirements, design, implementation, or testing. As an IDS CCB-approved change passes through each of these boards, a signature is required from both a NASA civil servant and a contractor in order to consider the life cycle phase complete.

A separate safety review panel determines the safety of Shuttle payloads. Software is one of many topics under the jurisdiction of the Payload Safety Review Panel (PSRP), but it represents one area of focus for payload safety. Software from the Shuttle's payload interfaces directly with Shuttle flight systems and software, and can therefore affect safety critical systems. The PSRP performs at least three phases of safety reviews: one which coincides with project requirements baseline, the next at design review, and a final certification review once verification has shown that all safety requirements have been met and that all safety controls and mitigations are in place and verified.

Key Observations: Control Boards

- Software control boards are an important aspect of managing software risks at the programmatic level and verifying software requirements implementation and compliance.
- Software control boards are project-specific and report directly to the program manager or to parent control boards.

Independent Assessment (NASA)

Independent Assessments (IA) are associated with OSMA, IV&V, and the Chief Engineer's Office, and are usually initiated by request from within a project, from a Center or Headquarters request, or from the Agency itself. For IV&V, IA is used to identify where a project's software may be weak and need additional analyses, processes, and verification. An IV&V IA outlines the minimum level of IV&V to be applied to systems, and it can be used to determine if and where further IV&V is needed on a project.

IAs can be performed at the project, program, Center, and Agency levels. For example, a recent IV&V IA was performed across NASA. Generally, an IA has a specific focus area, like Software Quality on the International Space Station. The newly created NASA Engineering and Safety Center (NESC) is also performing independent analyses and assessments on NASA Programs.

In addition, the Internal Process Assessments Office (IPAO) in the NASA Chief Engineer's Office evaluates programs for their budget, schedule, and technical progress.

Key Observations: Independent Assessment

- IV&V Independent Assessments (IAs) are used to identify where a program/project’s software may be weak and need additional analyses, processes, or verification.
- IAs can be performed at the program, project, Center, and Agency levels. The newly created NASA Engineering and Safety Center (NESC) is also performing independent analyses and assessments on NASA programs.

3.1.5 Certification Processes (NASA)

Software Assurance (NASA)

Although no formal software certification process is implemented, the totality of Software Assurance (SA) represents a de facto incremental certification process. SA consists of the disciplines of software quality, software reliability, software safety, software verification and validation, and independent verification and validation. These disciplines work together to form the software risk mitigation strategy for NASA's software. While NASA or even contractor SA organizations may not perform all the functions, analyses, processes, and procedures that make up these disciplines, they are responsible for ensuring that an appropriate amount of all software assurance processes are applied to a project according to its risk, complexity, and operational environment.

The purpose of SA is to make certain that software products are of high quality and operate safely. These include products delivered to and used within NASA, and products developed and acquired by NASA. SA assists in risk mitigation by minimizing defects and preventing problems and, through its activities, enables improvement of future products and services. SA is performed by various personnel at each Center in accordance with the organizational structure and governing documents for each program or project. All unresolved SA and risk issues are elevated to the level necessary for their resolution. SA is performed by both the acquirer and provider organizations.

The SA process is the planned and systematic set of activities that ensure conformance of software life cycle processes and products to requirements, standards, and procedures. The process confirms that software and its related products meet their specified requirements; conform to standards and regulations; are consistent, complete, correct, safe, secure and reliable as warranted for the system and operating environment; and satisfy customer needs. SA analyzes and ensures that all processes used to acquire, develop, assure, operate, and maintain the software are appropriate, sufficient, planned, reviewed, and implemented according to plan, and meet any required standards, regulations, and quality requirements. SA utilizes relevant project-based measurement data to monitor each product and process for possible improvements.

The SA disciplines can be thought of as an umbrella risk mitigation strategy for ensuring that a system is both safe and of the highest quality possible. The disciplines of software assurance are identified in Figure 9. Each discipline brings its own perspective to the tasks; the collective effect of all these efforts provides assurance of mission safety, reliability, and quality.

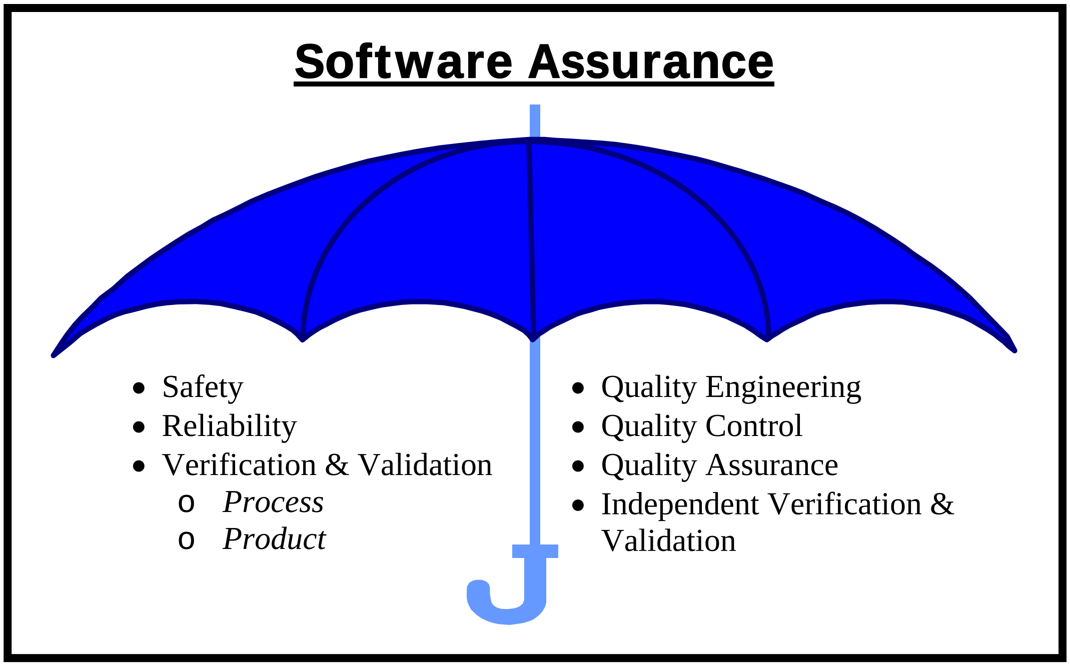


Figure 9. Software Assurance Umbrella.

Key Observations: Software Assurance

- Software Assurance (SA) consists of the disciplines of software quality, software reliability, software safety, software verification and validation, and independent verification and validation.
- The SA process is the planned and systematic set of activities that ensure conformance of software life cycle processes and products to requirements, standards, and procedures.
- SA disciplines can be thought of as an umbrella risk mitigation strategy for ensuring that a system is both safe and of the highest quality possible.

Certification Audits (NASA)

Certification audits of NASA software projects were not discussed to a significant extent during the NNBE software meetings mentioned in this report. This topic, specifically the Certification of Flight Readiness for the Shuttle, will be open to further discussion at a future date.

Certification Review Process (NASA)

The Shuttle Avionics Integration Lab (SAIL) is designed to emulate the avionics and software systems of all Space Shuttles in order to perform high-fidelity testing of new software and upgrades to existing systems. The facility represents the final set of system testing before on-board software is certified for flight. In the past, the SAIL has identified errors which could have resulted in a hazardous situation during a Shuttle mission.

The certification review process for NASA software projects was not covered completely during the NNBE software meetings mentioned in this report. This topic, in particular the Preliminary Acceptance Review and the Flight Readiness Review, is open to further discussion at a future date.

<u>Key Observations: Certification Review Process</u>

- The Shuttle Avionics Integration Lab (SAIL) represents the final set of system testing before software is certified for flight, and has identified errors which could have resulted in a hazardous situation during a shuttle mission.

3.2 Navy Software Development & Safety - Summaries and Key Observations

Software for the Navy's VIRGINIA Class Ship Control System, which is developed under the overall systems engineering process along with the rest of the Ship Control System, has been examined using the following framework:

3.2.1 Organization
3.2.2 Software Safety Requirements
3.2.3 Implementation Processes
3.2.4 Compliance Verification Processes
3.2.5 Certification Processes

Each section includes a narrative summary and key observations.

3.2.1 Organization (Navy)

Organizational Structure (Navy)

NAVSEA is the Navy Department's central activity for designing, engineering, integrating, building, and procuring U.S. Naval ships, weapons, combat systems, and other systems, including the software that control these systems. Additionally, NAVSEA provides technical, industrial, and logistics support for naval ships and ensures the proper design and development of the total ship, including contractor-furnished shipboard systems and associated software.

NAVSEA has defined Team Submarine as the organization responsible for submarine platform and system acquisition, in-service support, and modernization. As shown in Figure 10, the Program Executive Office (PEO) for Submarines is responsible for platform and system acquisition. The PEOs rely on technical support from the following NAVSEA organizations:

- SEA05 – Ship Design, Integration and Engineering,
- SEA07 – Undersea Warfare,
- NSWC – Naval Surface Warfare Center, and
- NUWC – Naval Undersea Warfare Center.

Software development at NAVSEA is conducted as an integral part of system development. The Program Office responsible for platform or system acquisition is also responsible for software acquisition for that platform and/or system. For example, PMS450 is the Program Office responsible for acquisition of the VIRGINIA Class Submarine, including the Ship Control System which is the focus of this report. The Program Manager is a uniformed Naval Officer, O-6 (Captain), who reports directly to the Program Executive Officer, Submarines (PEO SUB). PEO SUB is an Admiral who has responsibility for all submarine acquisition for the Navy.

While substantial support is provided by personnel located remotely at SEA05, SEA07, NSWC, and NUWC, significant support is provided by these organizations on-site in the Program Office.

The integration in the Program Office of personnel from these organizations and various support contractors is shown in the organizational chart for PMS450, the VIRGINIA Class Submarine Program Office (Figure 11).

In order to understand the software management process, it is essential to understand the organization. The VIRGINIA Class Submarine Program Office, PMS450, is organized into several sub-tier organizations, shown in Table 3 below. The “W” group consists solely of uniformed Navy personnel who are integrated into the Program Office to provide an on-going input from an operator’s perspective. The “T” group is charged with design and acquisition of Hull, Mechanical, and Electrical (HM&E) systems such as the diesel engine, the Trim and Drain system, the Ship Control System (SCS), and the hull coatings. Within the Program Office, systems can be acquired as Government Furnished Equipment (GFE) or Contractor Furnished Equipment (CFE) for contractual and/or core technical competency considerations. HM&E systems are primarily CFE.

Development of HM&E systems within PMS450T is accomplished via three groups. The Design Group, PMS450T1, is organized around System Integration Teams (SIT) charged with detailed design of a system, or with technical responsibility for a platform-wide technical area such as shock or acoustics. Development of each subsystem/component is conducted in an integrated fashion with both hardware and software managed by a single SIT. The Research and Development (R&D) group, PMS450T4, is responsible for development of new systems and major components. The R&D group is charged with transition of new technologies and maintaining appropriate budgets to implement the selected designs. Logistics products for all HM&E systems are the responsibility of personnel in the logistics group, PMS450TL.

Table 3. PMS 450 Roles & Responsibilities in the Software Management Process

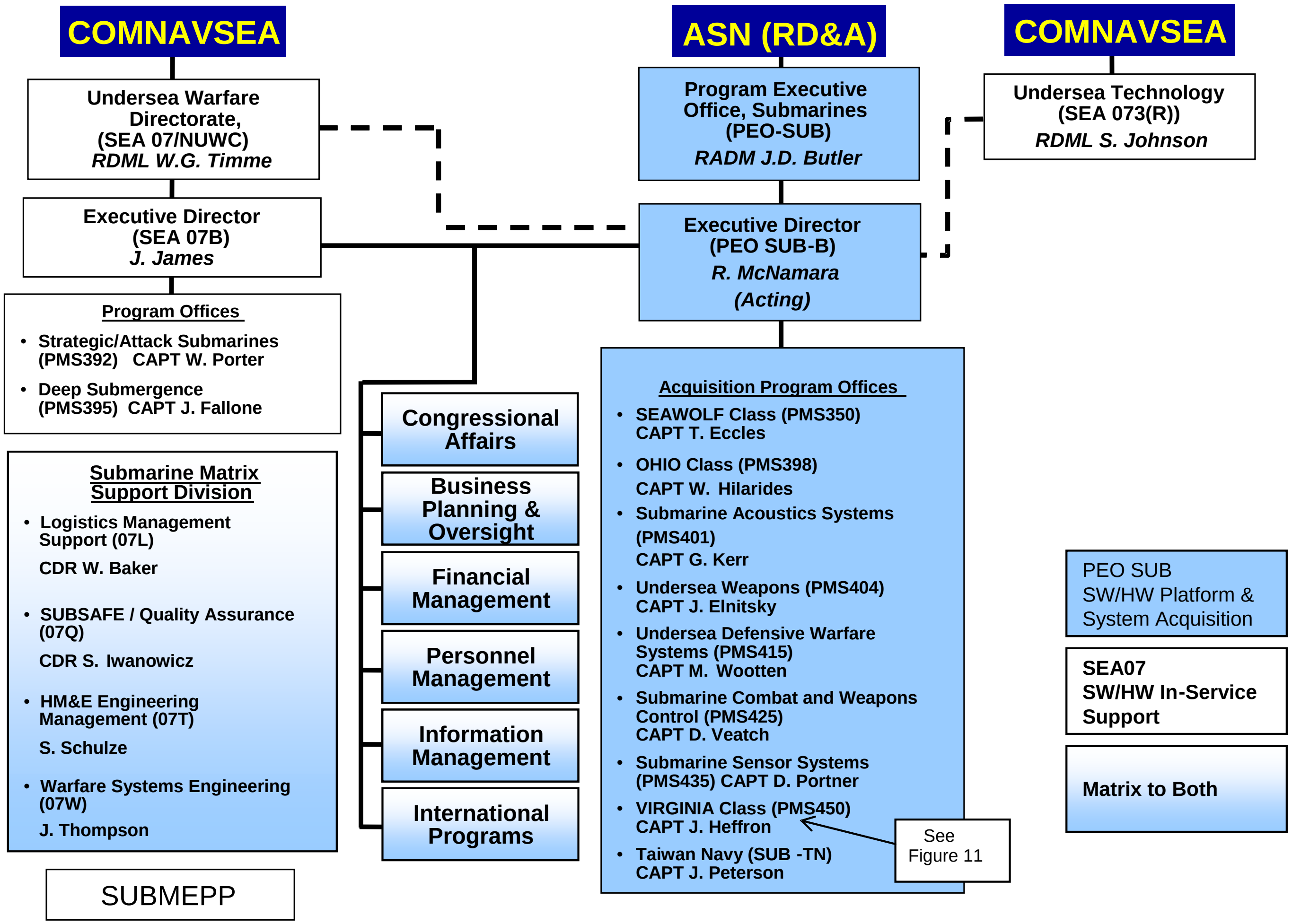
PMS 450 Sub-Tier Organization	Role in Software Management Process
W – Solely uniformed Navy Personnel	Operator Input
T – Mixture of Navy/Civilians	Design, Development & Acquisition of HM&E Systems
T1 – System Integration Teams	Design
T4 – R&D	Development
TL – Logistics	Logistical Support

Recently, the VIRGINIA Class Submarine Program Office, PMS450, has been re-organized to better support each delivered ship of the class as it enters service until it is formally transitioned to the care of the NAVSEA life-cycle manager approximately four years later. The charts and discussion in this report reflect the organization in existence prior to this re-organization. It is this organization with which the Program Office has accomplished the system and software development discussed.

Key Observations: Organizational Structure

- Software development at NAVSEA is conducted as an integral part of system development. The Program Office responsible for platform or system acquisition is also responsible for software acquisition for that platform and/or system.
- Development of each subsystem/component is conducted in an integrated fashion with both hardware and software managed by a single System Integration Team.

TEAM SUBMARINE ORGANIZATION



COMNAVSEA

Undersea Warfare Directorate, (SEA 07/NUWC)
RDML W.G. Timme

Executive Director (SEA 07B)
J. James

Program Offices

- Strategic/Attack Submarines (PMS392) CAPT W. Porter
- Deep Submergence (PMS395) CAPT J. Fallone

Submarine Matrix Support Division

- Logistics Management Support (07L)
  CDR W. Baker
- SUBSAFE / Quality Assurance (07Q)
  CDR S. Iwanowicz
- HM&E Engineering Management (07T)
  S. Schulze
- Warfare Systems Engineering (07W)
  J. Thompson

SUBMEPP

ASN (RD&A)

Program Executive Office, Submarines (PEO-SUB)
RADM J.D. Butler

Executive Director (PEO SUB-B)
R. McNamara
(Acting)

Congressional Affairs

Business Planning & Oversight

Financial Management

Personnel Management

Information Management

International Programs

Acquisition Program Offices

- SEAWOLF Class (PMS350)
  CAPT T. Eccles
- OHIO Class (PMS398)
  CAPT W. Hilarides
- Submarine Acoustics Systems (PMS401)
  CAPT G. Kerr
- Undersea Weapons (PMS404)
  CAPT J. Elnitsky
- Undersea Defensive Warfare Systems (PMS415)
  CAPT M. Wootten
- Submarine Combat and Weapons Control (PMS425)
  CAPT D. Veatch
- Submarine Sensor Systems (PMS435) CAPT D. Portner
- VIRGINIA Class (PMS450)
  CAPT J. Heffron
- Taiwan Navy (SUB -TN)
  CAPT J. Peterson

See Figure 11

COMNAVSEA

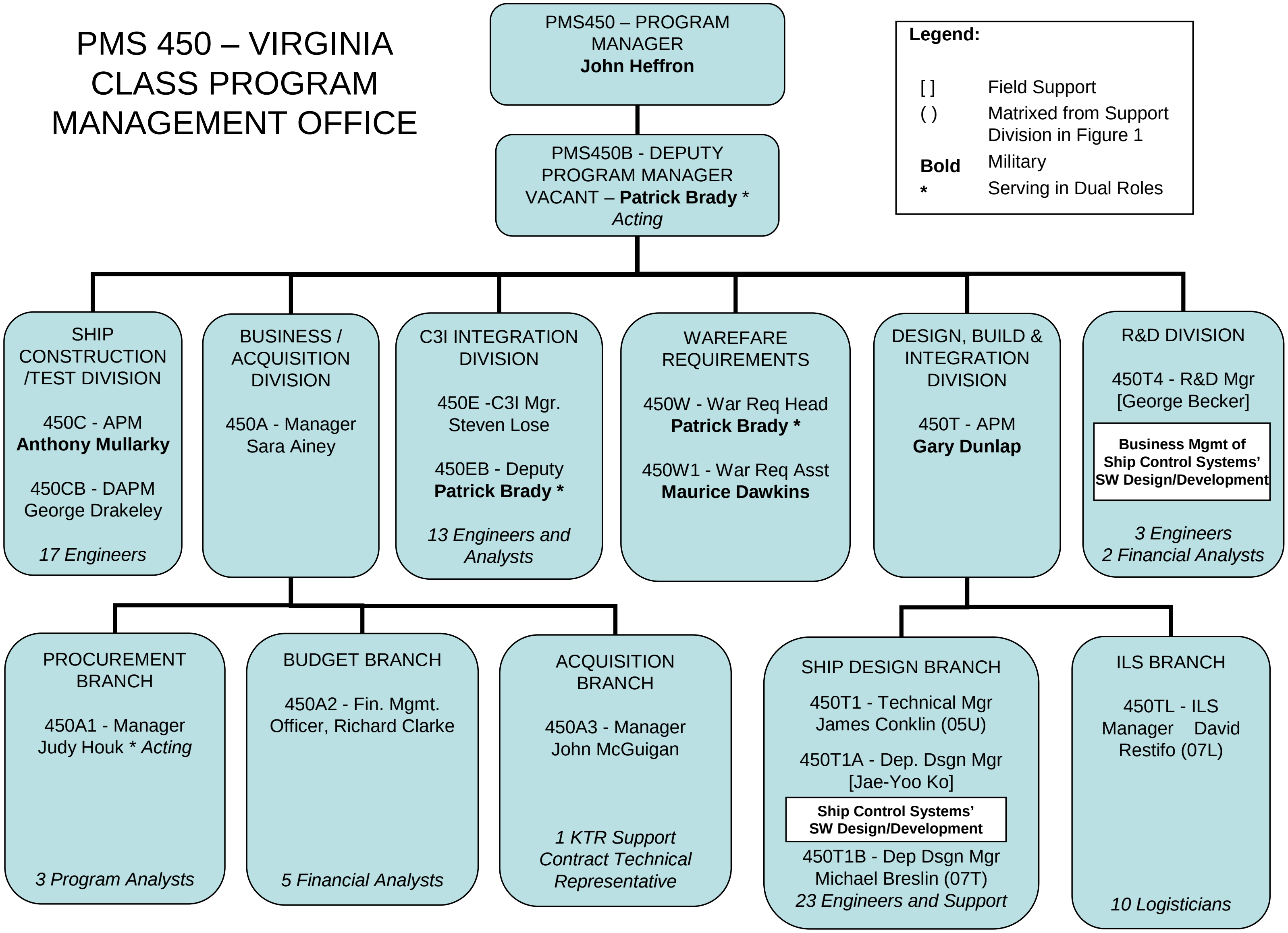
Undersea Technology (SEA 073(R))
RDML S. Johnson

PEO SUB SW/HW Platform & System Acquisition

SEA07 SW/HW In-Service Support

Matrix to Both

Figure 10. Organizations that Comprise Team Submarine.



PMS 450 – VIRGINIA CLASS PROGRAM MANAGEMENT OFFICE

PMS450 – PROGRAM MANAGER
John Heffron

PMS450B - DEPUTY PROGRAM MANAGER
VACANT – **Patrick Brady** * *Acting*

Legend:

[ ]	Field Support
( )	Matrixed from Support Division in Figure 1
Bold	Military
*	Serving in Dual Roles

SHIP CONSTRUCTION /TEST DIVISION
450C - APM
Anthony Mullarky
450CB - DAPM
George Drakeley
17 Engineers

BUSINESS / ACQUISITION DIVISION
450A - Manager
Sara Ainey

C3I INTEGRATION DIVISION
450E -C3I Mgr.
Steven Lose
450EB - Deputy
Patrick Brady *
13 Engineers and Analysts

WAREFARE REQUIREMENTS
450W - War Req Head
Patrick Brady *
450W1 - War Req Asst
Maurice Dawkins

DESIGN, BUILD & INTEGRATION DIVISION
450T - APM
Gary Dunlap

R&D DIVISION
450T4 - R&D Mgr
[George Becker]
Business Mgmt of Ship Control Systems' SW Design/Development
3 Engineers
2 Financial Analysts

PROCUREMENT BRANCH
450A1 - Manager
Judy Houk * *Acting*
3 Program Analysts

BUDGET BRANCH
450A2 - Fin. Mgmt. Officer, Richard Clarke
5 Financial Analysts

ACQUISITION BRANCH
450A3 - Manager
John McGuigan
1 KTR Support Contract Technical Representative

SHIP DESIGN BRANCH
450T1 - Technical Mgr
James Conklin (05U)
450T1A - Dep. Dsgn Mgr
[Jae-Yoo Ko]
Ship Control Systems' SW Design/Development
450T1B - Dep Dsgn Mgr
Michael Breslin (07T)
23 Engineers and Support

ILS BRANCH
450TL - ILS Manager David Restifo (07L)
10 Logisticians

Figure 11. PMS 450 Organization.

Technical Authority (Navy)

The responsibility for establishing and maintaining technical requirements is vested in the NAVSEA 05 organization, which organizes technical requirements by each major ship system. The technical authority is charged with that responsibility for all aspects of the system, including both hardware and software. Technical authority typically resides with the headquarters organization, though in some cases that responsibility has been delegated to a NAVSEA field activity. In many cases, hardware and/or software experts from NAVSEA field activities augment the headquarters staff, either on-site or remotely. For example, for the VIRGINIA Class Submarine Ship Control System, NAVSEA 05Z, Deputy for Integrated Design and Engineering, is the technical authority. Personnel from the Naval Surface Warfare Center, Carderock Division (NSWC, CD) based in Bethesda, Maryland, and Groton, Connecticut, provide additional expertise to NAVSEA 05.

Recently, NAVSEA headquarters established technical “warrant” holders. These warrant holders are recognized experts in their fields and are empowered to make technical decisions for NAVSEA in their warranted field; most warrant holders are in NAVSEA 05. The group lead in NAVSEA 05 is issued a technical warrant, and, as such, is personally accountable to the Chief Engineer (NAVSEA 05) for technical matters regarding systems in his/her charge. Programmatic decisions requiring Program Office letters typically include a counter-signature by the technical authority. The technical authority issues letters documenting technical decisions, often with Program Office counter-signature. There is no distinction in how the technical authority is managed for software versus hardware.

While there is an implicit understanding of the need for software competency at NAVSEA, there is no recognized software discipline per se. Software safety is further removed from recognition as a formal discipline. Warrants are primarily issued in domain areas like sonar or combat systems and not in areas like system and software development or software QA. Since warrants do not exist for these areas, neither software development nor software safety has a warrant holder.

Subsequent to the meetings and discussions documented in this report and based on observations from a NAVSEA survey of aviation industry fly-by-wire flight control systems, SEA07 and NAVSEA 05 issued the *Requirements Manual for Submarine Fly-By-Wire Ship Control Systems NAVSEA T9044-AD-MAN-010.* This manual addresses development, safety analysis, and certification of software-intensive ship control systems and could serve as a springboard for NAVSEA management to establish warrant holders for software development and software safety. The manual may also be the genesis of a platform level Safety of Flight Requirements Manual, which would represent a good start towards achieving standardization of software development and software safety practices at NAVSEA.

Key Observations: Technical Authority

- Software and hardware development are not recognized as formal and distinct disciplines; instead, the NAVSEA technical authority for software and hardware development is rolled into the technical authority as organized by each major ship system.

- Technical warrant holders are recognized experts in their fields and are empowered to make technical decisions for NAVSEA in their warranted field. As such, warrant holders are personally accountable to the Chief Engineer (NAVSEA 05) for technical matters regarding systems in their charge.
- Although warrant holders currently do not exist for disciplines such as software development or software safety, development of the *Requirements Manual for Submarine Fly-By-Wire Ship Control Systems* may result in establishment of these warrant holders.

Human Resources (Navy)

The issuance of the *Requirements Manual for Submarine Fly-By-Wire Ship Control Systems NAVSEA T9044-AD-MAN-010* may drive the creation of positions formally designated as responsible for software or software safety. The manual mandates an organization within NAVSEA responsible for FBW SCS development and Certification compliance to this manual. SEA 07 has been designated to implement these requirements and assess compliance. SEA 05 (specifically SEA 05Z5) is responsible for the maintenance of the technical requirements. Supporting organizations and responsibilities are defined; since the manual mandates several types of audits and each relevant organization within the command will be required to maintain a certain number of qualified auditors for nomination, personnel will need to become qualified for these audits. Additional resources, or re-prioritization of existing resources, may be required to support these activities.

Procurement (Navy)

Overall procurement of the submarine is the responsibility of the Program Office, with the exception of propulsion plant equipment and systems procured by Naval Reactors. Because software is considered an integral part of developed or delivered systems, responsibility for software procurement follows system development and procurement.

DoD acquisition lifecycle policy emphasizes a process in which a command has oversight accountability for a system from concept to final disposition of its assets – the so-called "cradle-to-grave" process. On large, complex Navy platforms with low safety mishap tolerances, the same technical and quality assurance personnel who supported the acquisition program office also support the in-service and program offices for periodic certification and approval. This continuity is beneficial to software maintenance and software safety.

The VIRGINIA Class submarine program's concept was developed by using the best applications developed under previous submarine programs, using lessons learned, and establishing creative approaches to enhance and streamline processes. The result is the ability to design and build better submarines for lower costs.

The initial design contract was awarded in January 1996 as an Integrated Product and Process Development (IPPD) contract. This approach teamed representatives from the prime contractor, Electric Boat, their major subcontractor, Newport News Shipbuilding, and the government to establish design/build teams wherever benefits may exist. Teams included representatives, as required, for engineering, software development, construction, planning, logistics, test, quality, materials, purchasing, finance, and program management. This IPPD approach promoted effective communications and ensured optimum product-related decisions for ship design and construction, as well as risk management and mitigation. The IPPD approach also supported effective integrated ship/module construction, test, and outfitting, including the associated software systems.

Key Observations: Procurement

- Software is provided as an integral part of developed or delivered ship systems. The Program Office is responsible for ensuring a sufficient budget for software development and software safety. The Program Office responsibility for software procurement follows ship system development and procurement.
- Having the same technical and quality assurance personnel who supported the acquisition program office also support the in-service and disposition program offices provides continuity and benefits software maintenance and software safety.
- The Integrated Product and Process Development (IPPD) contract approach benefits software development and software safety associated with the ship systems. Establishing combined government and contractor design/build teams promotes effective communications and ensures optimum decisions for product design/construction, risk management, and risk mitigation.

3.2.2 Software Safety Requirements (Navy)

Safety Philosophy (Navy)

The Submarine Safety (SUBSAFE) and Deep Submergence Systems (DSS) programs are primarily hardware oriented but, because of a strong commitment to safety ingrained at all levels of the submarine community by SUBSAFE and DSS scope of certification, software safety is also given strong emphasis. Even the general philosophy of emphasizing safety carries over to software systems, despite the lack of a standard corporate policy for software safety processes and techniques. The recently adopted *Requirements Manual for Submarine Fly-By-Wire Ship Control Systems* provides a significant improvement by institutionalizing a process-driven philosophy for software development and software safety.

The safety philosophy for the VIRGINIA Class Submarine was to impose maximum responsibility and provide commensurate authority to Electric Boat (EB) for development of HM&E systems, including the ship control system. The safety analysis was conducted by EB and approved by the Navy Program Manager and Technical Authority. With the issuance of the software safety criteria by the Certification Process Action Team (Cert PAT), the MIL-STD-882 analysis was re-oriented to heavily emphasize analysis of the system software. The Cert PAT invoked software safety criteria for the ship control system that must be met in order for the system to be considered safe for submerged operations. A team of Navy subject matter experts and stakeholders developed these criteria. For both the SEAWOLF and VIRGINIA ship control systems, safety analysis was performed on the designed system; it was not part of the system design process per se. Such after-the-fact analyses may not be optimal for either effectiveness or efficiency. NAVSEA has addressed this by developing a set of unique requirements for certification of fly-by-wire ship control systems. These requirements are based on observations from a NAVSEA survey of aviation industry fly-by-wire flight control systems accomplished over the last three years. The Safety of Flight industry survey team’s observations were provided to NASA in the course of this phase of the NNBE effort.

Both the Navy and EB recognized the critical nature of the VIRGINIA Class Ship Control System and took numerous actions to reduce risk. EB willingly imposed stricter discipline in their software development process in order to build in quality. These efforts were recognized when EB used the Ship Control System development as a basis for earning an SEI CMM rating of Level 3. The Navy funded the Software Program Managers Network (SPMN) to train EB on formal inspections to improve safety defect discovery. The SPMN software program manager’s “control panel” was implemented early on with heavy emphasis on principles of managed turnover, no secrets, earned value measurement, and meaningful metrics. These principles require the developer to anticipate and actively address personnel turnover, ensure program issues and problems are faced head on instead of buried in hopes they disappear, constantly measure and track the value of work accomplished to the work planned, and identify measures of effectiveness that allow for early and meaningful management actions. The Navy required numerous proof-of-concept demos in order to aggressively manage risk, including safety aspects. These included two demonstrations of the fault tolerant processing system architecture and three Concept of Operations Exercises (COOPEXes) in which uniformed Navy operators “drove” an engineering development model of the VIRGINIA Ship Control Station on a motion platform. Tactical Digital Standards (TADSTANDS) for items such as processor usage were imposed with EB accession to provide a disciplined yardstick by which to measure success. EB and the Navy agreed to a concurrent engineering approach whereby multiple builds would be used for an incremental development with formal entrance and exit criteria. Strong IV&V onsite was used to help quickly dispel requirements fog. Lastly, under the new warrant holder corporate policy, the Navy is shifting away from the Cert PAT process to a more standardized approach built around a requirements manual with tech authority/warrant holders' approval.

Key Observations: Safety Philosophy

- No formal NAVSEA institutional doctrine on software safety yet exists, but the safety philosophy ingrained in the submarine community carries over to software systems.
- The recently adopted *Requirements Manual for Submarine Fly-By-Wire Ship Control Systems* institutionalizes a process-driven philosophy.
- Software safety criteria identified by the Cert PAT define assertions that the system software must not do in order to be considered safe within the defined submerged operating envelope.
- Key principles for successful software development include managed turnover, no secrets, empowered individuals, earned value, metrics, and IV&V.

Governing Documents (Navy)

New design software development is governed by the same high-level documents as overall system design. The DoD 5000 series of documents identifies mandatory and preferred processes for defense systems acquisition. At the time the VIRGINIA Class Submarine program was begun, DoD 5000 required the use of DoD-STD-2167/2167A for system development and MIL-STD-2168 for Quality Assurance. Shortly after the award of the VIRGINIA design contract, DoD imposed MIL-STD-498 (jointly issued as commercial standard IEEE/EIA 12207) for software development. However, the VIRGINIA design contract was awarded at the height of the DoD Acquisition Reform movement, which discouraged imposition of such standards. Instead, use of contractor's best practices was encouraged in procurements. Acquisition Reform did allow for use of standards where the contractor proposed such. For the VIRGINIA Class Ship Control System, the lead design yard proposed DoD-STD-2167A because of their familiarity with it. Currently, the DoD 5000 series recommends allowing the contractor to use their own best practice(s) for software development upon approval by the Navy.

Despite the DoD move away from military and Department of Defense Standards, VIRGINIA Class Ship Control development was continued under the DoD-STD-2167A process by unanimous agreement of the Program Office, Technical Authority, and lead design yard, EB. The organizations agreed that maintaining the DoD-STD-2167A framework ensured that all aspects of the system and software development would receive appropriate scrutiny and formality. A safety analysis per MIL-STD-882C, leveraging aspects of STANAG-4404, was also required. During the system development, significant tailoring was done to MIL-STD-882C in order to focus the analysis on software and elimination of specific identified hazards. At the start of the VIRGINIA Class Ship Control System development, DoD 5000 recommended the use of the SEI CMM rating as a source selection criterion but did not mandate it as does the current 5000 series. The Program Office did not impose a CMM rating on the contractor for source selection.

Key Observations: Governing Documents

- New design software development is governed by the DoD 5000 series of documents that identify mandatory and preferred processes for defense systems acquisition. DoD 5000 currently recommends allowing the contractor to use their own best practice for software development upon approval of the Navy.
- The Program Office, Technical Authority, and lead design yard (EB) unanimously agreed to implement the VIRGINIA Class Ship Control System under the DoD-STD-2167 process.
- During the system development, significant tailoring was done to the safety analysis requirements document, MIL-STD-882C, in order to focus the analysis on software and ensure that specific identified hazards did not exist.

Safety Requirements (Navy)

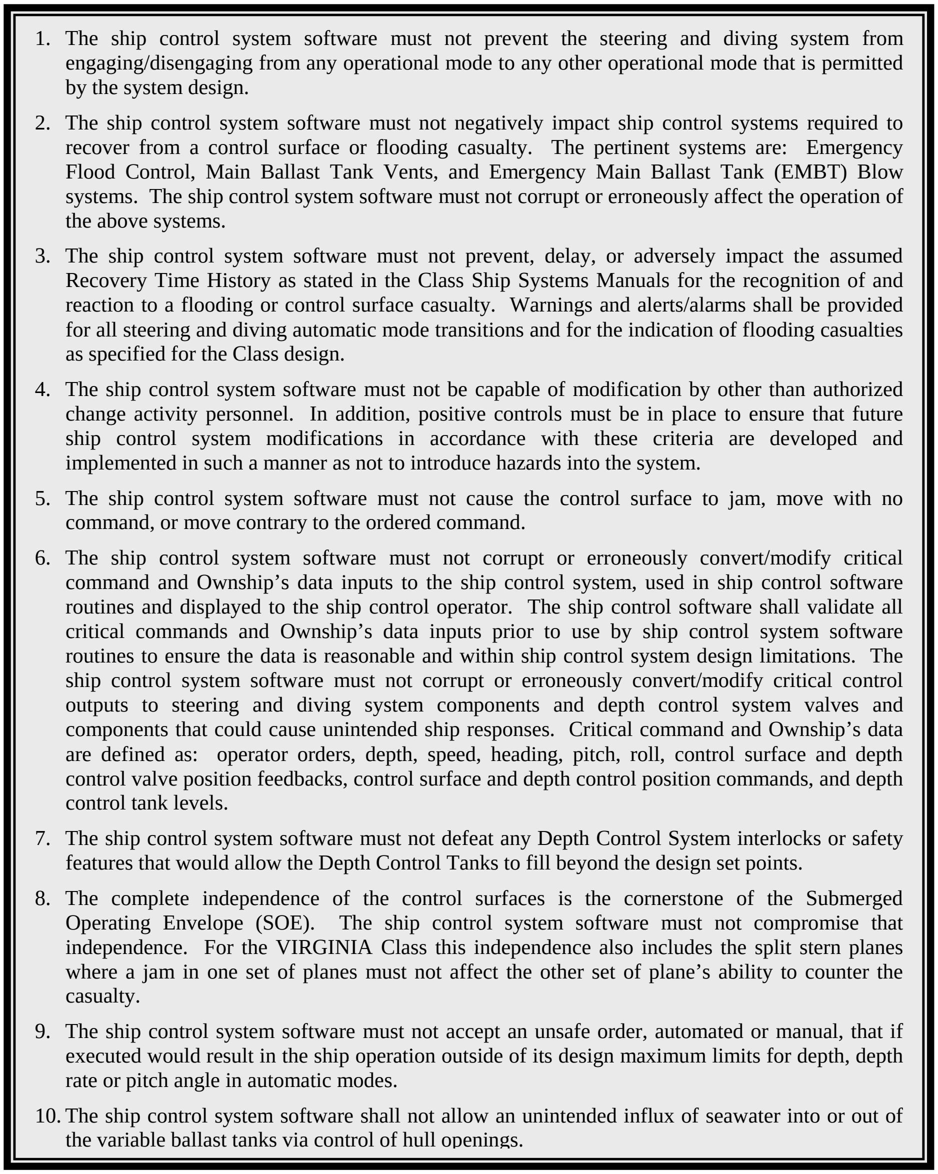
The Specification for Building Submarines (commonly referred to as the "Ship Spec") identifies the requirements for a ship safety program as defined in the Ship Safety Description Document (SSDD). There are no safety specific system or software requirements, per se, but system functional requirements which support safe operation of the ship enable the ability to certify that the specified Operational Availability (A_o) is identified throughout the requirements documentation.

For VIRGINIA Class, the SSDD identifies eighteen new or significantly modified systems for a safety analysis per MIL-STD-882. The Ship Control System was identified for a safety analysis in the SSDD because it is a new design system. However, there was no platform level (submarine) safety analysis required, nor was one conducted.

The SEAWOLF was the first Navy nuclear submarine with a true fly-by-wire, software intensive Ship Control System. Though initially planned, as part of a general down-scoping of requirements during the design phase, the SEAWOLF program deleted the requirement for a safety analysis of the Ship Control System. As part of achieving initial certification of the SEAWOLF Class submarines, NAVSEA elected to use an existing certification advisory panel, the SEAWOLF Class Cert PAT, to oversee certification of the Ship Control System. This process included identification of twelve (12) software safety criteria against which the SEAWOLF Ship Control System was evaluated. Objective quality evidence (OQE) demonstrating compliance with the criteria was required. Because the VIRGINIA Class Ship Control System implements an even more software intensive design which removes the mechanical-hydraulic backup present on SEAWOLF, the VIRGINIA Class Cert PAT took on the responsibility to oversee the certification of the VIRGINIA Class Ship Control System. This team identified ten of the SEAWOLF safety criteria as applicable to the VIRGINIA Class.

These criteria, shown in Figure 12, were imposed on the lead design yard, EB, as system specification requirements.

The Cert PAT evaluation for the SEAWOLF Ship Control System was implemented after the fact on the as-designed system. For the VIRGINIA Class, the safety analysis was planned and began execution during system design. However, due to multiple significant revisions of the safety analysis process, the adjudicated analysis process was performed on the as-designed system. Such “after the fact analyses” may not be optimal for either effectiveness or efficiency. NAVSEA addressed this in the recently adopted *Requirements Manual for Submarine Fly-By-Wire Ship Control Systems* to document requirements for development, safety analysis, and certification of software intensive fly-by-wire ship control systems.



1. The ship control system software must not prevent the steering and diving system from engaging/disengaging from any operational mode to any other operational mode that is permitted by the system design.
2. The ship control system software must not negatively impact ship control systems required to recover from a control surface or flooding casualty. The pertinent systems are: Emergency Flood Control, Main Ballast Tank Vents, and Emergency Main Ballast Tank (EMBT) Blow systems. The ship control system software must not corrupt or erroneously affect the operation of the above systems.
3. The ship control system software must not prevent, delay, or adversely impact the assumed Recovery Time History as stated in the Class Ship Systems Manuals for the recognition of and reaction to a flooding or control surface casualty. Warnings and alerts/alarms shall be provided for all steering and diving automatic mode transitions and for the indication of flooding casualties as specified for the Class design.
4. The ship control system software must not be capable of modification by other than authorized change activity personnel. In addition, positive controls must be in place to ensure that future ship control system modifications in accordance with these criteria are developed and implemented in such a manner as not to introduce hazards into the system.
5. The ship control system software must not cause the control surface to jam, move with no command, or move contrary to the ordered command.
6. The ship control system software must not corrupt or erroneously convert/modify critical command and Ownship’s data inputs to the ship control system, used in ship control software routines and displayed to the ship control operator. The ship control software shall validate all critical commands and Ownship’s data inputs prior to use by ship control system software routines to ensure the data is reasonable and within ship control system design limitations. The ship control system software must not corrupt or erroneously convert/modify critical control outputs to steering and diving system components and depth control system valves and components that could cause unintended ship responses. Critical command and Ownship’s data are defined as: operator orders, depth, speed, heading, pitch, roll, control surface and depth control valve position feedbacks, control surface and depth control position commands, and depth control tank levels.
7. The ship control system software must not defeat any Depth Control System interlocks or safety features that would allow the Depth Control Tanks to fill beyond the design set points.
8. The complete independence of the control surfaces is the cornerstone of the Submerged Operating Envelope (SOE). The ship control system software must not compromise that independence. For the VIRGINIA Class this independence also includes the split stern planes where a jam in one set of planes must not affect the other set of plane’s ability to counter the casualty.
9. The ship control system software must not accept an unsafe order, automated or manual, that if executed would result in the ship operation outside of its design maximum limits for depth, depth rate or pitch angle in automatic modes.
10. The ship control system software shall not allow an unintended influx of seawater into or out of the variable ballast tanks via control of hull openings.

Figure 12. Virginia Class Ship Control System Software Safety Criteria

Key Observations: Safety Requirements

- The Ship Spec identifies the requirement for a ship safety program with new or significantly modified systems for a safety analysis per MIL-STD-882.
- A Certification Process Action Team (Cert PAT) identified software safety criteria for evaluation of the VIRGINIA Class Ship Control System. The associated system safety analysis was significantly modified to focus on these criteria while still retaining the basic MIL-STD-882 approach.
- The *Requirements Manual for Submarine Fly-By-Wire Ship Control Systems* may supersede the need for the Cert PAT to address Ship Control Systems.

Requirements Flow Down (Navy)

Navy submarines are procured using multiple requirements documents starting at the mission level and flowing down to the hardware and software component level. At the earliest stage of a program, a “Mission Area Focused” Capabilities Based Document is defined, identifying a service need. An Operational Requirements Document (ORD) identifies the highest platform level requirements (Note: The DoD 5000 series of documents in effect at the time the VIRGINIA Program was initiated required an ORD, while the current version requires an Initial Capabilities Document (ICD)). The Ship Spec captures system level requirements for the entire submarine at a level of detail sufficient to begin contracting action for system and component design work. The Ship Spec includes sections on major subsystems and attributes which will be at the center of concept, preliminary, and detail design activities. These requirements then flow to Ship Control System design documents, which include:

- System/Segment Specification per DoD-STD-2167A,
- Software Requirements Specifications (SRSs) and Software Detailed Design Documents (SDDDs) for each Computer Software Configuration Item (CSCI),
- Prime Item Development Specifications (PIDSs) for each Hardware Configuration Item (HWCI),
- Interface Requirements Specifications (IRSs)/Interface Design Specifications (IDSs) for system level interfaces, and
- Interface Requirements Table (IRT) for internal Ship Control System interfaces.

Key Observations: Requirements Flow Down

- System specific requirements are first identified at the Ship Spec level and are then flowed down and imposed on the contractor throughout the system design documentation.

Requirements Ownership (Navy)

The NAVSEA technical authority is the “owner” of the platform and system functional requirements for new design systems, including the software associated with those systems. NAVSEA 05 is the technical authority and therefore the owner of the Ship Control System functional design requirements for the VIRGINIA Class Ship Control System. The ORD and Ship Spec are Navy-generated and Navy-owned requirements documents. The Ship Control System Specification, SRSs, and lower tier requirements documents are generated and proposed by EB for the Ship Control System, and approved by the Navy. These documents are maintained under tight configuration management throughout the design process, and into the lifecycle maintenance phase. Requirements that must be formally verified during the system Functional Configuration Audit (FCA) are designated by the word “shall” and given a unique number for tracking. Derived requirements that are identified by the developer based on the formal requirements are not formally verified. The software safety criteria for evaluation in the system safety analysis were imposed on EB via formal letter authored by Technical Authority and concurred with by the Program Office.

Key Observations: Requirements Ownership

- The NAVSEA technical authority is the “owner” of the platform and system functional requirements for new design systems, including the software associated with those systems.
- Software safety criteria are imposed on the contractor by the technical authority via a formal process with concurrence of the Program Office.

3.2.3 Implementation Processes (Navy)

Concept Development (Navy)

Concept development for the VIRGINIA Class Submarine Ship Control System was accomplished at the system level and centered around functional requirements. The selection of a software-based, fault-tolerant processing system for ship control was made during concept development to support the system level functional requirements. Numerous evaluations, exercises, proof-of-concept demonstrations, and various technical studies were all done to support functional requirements as opposed to safety requirements. Software is developed under the overall systems engineering process along with the rest of the Ship Control System. Wherever possible, early proof-of-concept efforts include software.

Examples include proof-of-concept testing for the software based fault tolerant processing system on prototype processing hardware and a Concept of Operations Exercise (COOPEX) for the man-machine interface of the Ship Control Station using software prototypes of the tactical design displays and controls. High level functions were partitioned between hardware and software per standard systems engineering practice. Similar partitioning was accomplished among Computer Software Configuration Items (CSCIs) within the totality of the system software.

Because of concerns about obsolescence and the anticipation of technology refresh, the design of the VIRGINIA Class submarine Ship Control System software included features to insulate the applications from an ever-changing Commercial-Off-The-Shelf (COTS) hardware and software environment. These features include Application Interfaces (APIs) between software modules, including the COTS operation system and processor Basic Input/Output System (BIOS). During the concept development phase, a modular design approach was used extensively to contain anticipated changes.

Key Observations: Concept Development – Navy

- Concept development for the VIRGINIA Class Submarine Ship Control System was accomplished at the system level and centered around functional requirements and not specified safety requirements.
- Early during the concept development phase of the VIRGINIA Class submarine Ship Control System, a modular software design approach was used extensively to contain anticipated hardware/software changes and address concerns about obsolescence.

Safety Analysis (Navy)

A MIL-STD-882 systems safety analysis was begun in the early stages of the VIRGINIA Class Ship Control System development with the conduct of a Preliminary Hazard Analysis during the Preliminary Design phase. The software safety criteria, the MIL-STD-882 analysis, developed by the Cert PAT, was modified to focus on software-oriented analysis. The primary objective of this analysis was to demonstrate that the Software Safety Criteria had been met and to provide the confidence needed for the safe operation of the ship control system.

The final analysis process was the result of a number of attempts to develop a cost effective safety analysis which would nonetheless provide the confidence needed to certify the operation of the ship control system as safe. The process was briefed twice to the Software System Safety Technical Review Panel (SSSTRP) of the Weapon System Explosives Safety Review Board (WSESRB), the Navy's premier weapons safety organization. Due to delays in defining an appropriate process, the safety analysis was conducted on software whose design was complete and for which coding had begun. The Navy realizes the technical and programmatic benefits to accomplishing the safety analysis as an integral part of the system development and is addressing this issue as part of the response to the Safety of Flight team's findings.

The VIRGINIA safety analysis began by establishing the ten software safety criteria shown in Figure 12 as the basis for declaring the software safe. The software safety criteria invoked by the Cert PAT define the performance boundaries for the system software to be considered safe within the defined submerged operating envelope. From these criteria, hazards were identified and grouped to minimize redundancy. Intermediate and lower level causative events that would lead to the hazard were derived using a fault tree analysis of the software. Verification requirements were then established stating actions required to determine if deficiencies exist in the software.

The software safety engineers analyze the software at the lowest level by evaluating strings of computer software units in a call tree for occurrence of any of the lowest level causative events. When verification requirements are met, the associated causative events did not occur. When all causative events do not occur, then the hazards do not exist. When all hazards in a group do not exist, then the hazard group does not exist. When all hazard groups do not exist, the software safety criterion is met. Finally, when all ten software safety criteria are met, the software is declared safe.

When verification requirements are not met, the deficiencies are documented as a violation of software safety criteria. The result is a must-fix problem trouble report. Developers and Navy management approve mitigation of hazards by designing the causal factors out of the implemented design totally or to a level of risk that is acceptable to Navy management, depending on the level of residual risk. The residual risk may then be mitigated by procedure, caution/warnings, safety interlocks, or other means. It is not necessary to eliminate all hazards, but it is necessary to mitigate any hazards to an acceptable level of risk. Any ideas that identify opportunities to increase safety are also documented. The safety analysis also includes a functional analysis using a checklist based on recommended analysis areas from the Joint Services Safety Certification (JSSC) Software System Safety handbook, a best practice review based on established safety coding guidelines from STANAG 4404, and a requirements traceability analysis to verify traceability up and down the hierarchy of requirements documents.

Software identified as safety critical via safety analysis is labeled as such in the header for each such software unit (Note: Due to the multiple re-starts of the safety analysis program, the effort to identify and label safety critical software units was aborted and is now being completed after the software has been delivered). Since the maintainers will be able to identify safety critical code in the source code itself, software maintenance will be improved. As with all highly complex software intensive systems, complete path testing is not practical. For the VIRGINIA Class SCS, a requirement of 100% statement coverage was set for all safety critical software units. Non-safety critical units had a goal of 100% statement coverage. In practice, most received 90% statement coverage.

Key Observations: Safety Analysis

- A MIL-STD-882 system safety analysis was begun in the early stages of the VIRGINIA Class Ship Control System development. The software safety criteria, the MIL-STD-882 analysis, developed by the Cert PAT, was modified during detailed design to focus on software-oriented analysis.
- Unmet verification requirements are documented as deficiencies, resulting in a must-fix problem trouble report.

Design Tools and Techniques (Navy)

Software is developed under the overall Systems Engineering process, along with the rest of the Ship Control System. Wherever possible, early proof of concept efforts included software. Examples include proof of concept testing for the software based fault tolerant processing system on prototype processing hardware, and a COOPEX for the man-machine interface of the Ship Control Station using software prototypes of the tactical design displays and controls. High level functions were partitioned between hardware and software per standard systems engineering practice. Similar partitioning was accomplished amongst Computer Software Configuration Items (CSCIs) within the totality of the system software.

The Ship Control System project utilized real-time structured analysis techniques for requirement development. The requirement specifications are in accordance with DOD-STD-2167A. The TEAMWORK CASE tool was utilized. The design approach was the Ada Design Approach for Real Time Systems (ADARTS) supported by the Software Productivity Consortium. This approach emphasizes the critical design and performance threads.

Software development tools included the *Continuus* configuration management and process management tools to enforce the Ship Control Development Process. The configuration management activity of the Navy's software development program provides a means of controlling access to software development files, and the change control process ensures that only technically sound software is released for test. In addition, the safety analysis program also identifies safety critical software at the unit level and provides a notation in the unit header that identifies the unit as safety-critical. This identifier is an indication to the software lifecycle maintainer that a safety analysis must be performed on the unit if it is changed.

The Ada and C CAST tools were used for unit tests. These tools provide assistance in developing unit test cases, documenting the results, and analyzing the test coverage. The Ship

Control software is primarily developed in Ada and utilized the Greenhills Multi Environment for Ada and C CAST. Compilers from AONIX and HP were used as well.

Key Observations: Design Tools and Techniques

- The Ship Control Project utilized real-time structured analysis techniques for requirement development, included a design approach that emphasizes the critical SW design and performance threads, implemented software configuration management and control processes, and employed software tools for developing unit test cases, documenting results, and analyzing test coverage.

Risk Management (Navy)

PMS450, the VIRGINIA Class Submarine Program Office, has an active risk management program for all program risks, including software. The VIRGINIA Class Risk Management Plan was developed to provide general guidance on risk management and to provide more specific guidance on one-time risk assessments. The program's Risk Process Description document defines the process in detail. Each system or functional area lead is responsible for identifying risks and mitigation strategies. As such, he or she is designated the Risk Area Manager (RAM) for each item. These risks and strategies are documented in a central risk database. The office has designated one individual to serve as the program's risk manager. This individual works with the RAMs to ensure periodic updates and timely closures of these risks. This process has been in place since preliminary system design and will remain active for the life of the Program Office.

Specific risk areas addressed for the Ship Control System include:

- Software developer staffing and experience,
- Delivery of Government Furnished Information (GFI) automatic control algorithms,
- Software developer staffing levels,
- Budget and schedule for software code and unit test, and
- Qualification and staffing level of software safety engineers performing the software safety analysis.

As required by the VIRGINIA Class Risk Management Plan, one or more mitigation plans were identified for each risk. Risks are retired as they are mitigated or realized and corrected. For VIRGINIA SCS, all risks were mitigated successfully except one, which is pending – the safety analysis task. This risk has been difficult to mitigate due to the lack of a standard software safety analysis method for non-weapons HM&E systems and multiple revisions to the safety analysis approach. (Note: This risk was considered successfully mitigated upon the completion of safety certification for the Ship Control System.)

Both the Navy and EB recognized the critical nature of the VIRGINIA Class Ship Control System and took multiple actions to reduce risk. The Navy required numerous proof-of-concept-demos in order to aggressively manage risk, including safety aspects. EB willingly imposed stricter discipline in their software development process in order to build in quality. These efforts were recognized when the Ship Control System development was a primary participant in earning an SEI CMM rating of Level 3 for EB. The Navy funded the Software Programmers Network (SPMN) to train EB on formal inspections to improve safety defect discovery. The Navy-accepted *Practical Software Measurement* approach was implemented. Using this issue driven approach, the development team identified program and technical issues, and selected specific quantifiable measures to track the status and progress of issues. Tactical Digital Standards (TADSTANDS) for items such as processor usage were imposed with EB accession to provide a disciplined yardstick by which to measure success. Lastly, the Navy and EB agreed to a concurrent engineering approach whereby multiple builds would be used for an incremental development with formal entrance and exit criteria.

Key Observations: Risk Management

- PMS450 has an active risk management program for all program risks, including software. As required by the VIRGINIA Class Risk Management Plan, one or more mitigation plans were identified for each risk.
- Each system or functional area has a Risk Area Manager (RAM) responsible for identifying risks and mitigation strategies, which are documented in a central risk database and tracked by the program's risk manager.
- The EB development team implemented the Navy-accepted *Practical Software Measurement* approach to reduce risk by identifying program and technical issues, and selecting specific quantifiable measures to track the status and progress of issues.

Work Management (Navy)

PMS450 operates in an IPPD environment where each system development has a Navy lead in the Program Office. Development of each subsystem/component is conducted in an integrated fashion with both hardware and software managed by a single System Integration Team (SIT). In general, the Navy lead for each SIT is an expert in the system under development who is matrixed in from a NAVSEA headquarters technical code or Navy field activity.

For Ship Control Systems, the Navy lead is a system expert from NSWC in Carderock, MD. Many Program Office personnel are required to achieve level III (highest) certification under the Defense Acquisition Workforce Improvement Act in one of a number of specific areas. The Ship Control System SIT leader is certified in Systems Planning, Research, Development, and Engineering (SPRDE), which includes coursework in software acquisition management.

The VIRGINIA Ship Control System Navy lead co-chairs the SIT with a contractor counterpart from EB, the lead design yard. EB is responsible for total system design and was the primary software developer. Automatic control algorithms are developed by NSWC and provided to EB as government furnished information (GFI). Software IV&V is performed by a Navy team lead by the NSWC, and includes NUWC and contractor personnel. Unlike traditional "Independent" V&V, this effort is conducted as part of the SIT process in an IPPD environment, and thus is less than fully independent.

Tasking to EB, Navy field activities, and directly supporting contractors is done annually via Individual Task Management Plans (ITMPs). This tasking can range in magnitude from a few man-months of activity to many millions of dollars, depending upon the size, complexity and specificity of the task. For the Ship Control System, EB is tasked by work breakdown structure, resulting in a single software development task and a single system/software safety analysis task each year. The VIRGINIA Ship Control System safety effort has its own ITMP.

Because of the safety-of-ship critical nature of the Ship Control System, a Safety Integrated Product Team (IPT) was established and charged with specific responsibility to ensure the safety analysis was properly conducted. The IPT includes members from the Program Office, EB, NSWC and support contractors, and SEA07 personnel. SEA07 personnel include representatives from the technical group and the SUBSAFE group. SEA07 is involved because of their critical role in certifying the ship for initial at-sea operation, their role as the technical authority for in-service submarines, and their role as leads for the SUBSAFE program. NAVSEA imposed maximum responsibility and provided commensurate authority to EB for development of the Ship Control System. The safety analysis was conducted by EB and approved by the Navy Program Manager and Technical Authority.

Key Observations: Work Management

- Development of each subsystem/component is conducted in an integrated fashion with both hardware and software managed by a single System Integration Team.
- Virginia Class Software IV&V has been conducted by the Navy as part of the SIT process in an Integrated Process and Product Team environment. The Navy was team-led by NSWC and included NUWC and contractor personnel.
- Tasking of System (SW/HW) supporting tasks to EB, Navy field activities, and directly supporting contractors is done annually by the Program Office via Individual Task Management Plans (ITMPs).
- Because of the safety-of-ship critical nature of the Ship Control System, a Safety Integrated Product Team (IPT) was established and charged with specific responsibility to ensure the safety analysis was properly conducted.
- Metrics collected from the inspections process are used to identify inspection process outliers. This data is used to determine if a unit should undergo additional inspections, or if there is a systemic problem.

3.2.4 Compliance Verification Processes (Navy)

Quality Assurance (Navy)

The VIRGINIA Class Lead Design Yard, EB, conducts a separate and distinct software quality assurance activity as part of their software design process. Audit findings are reported directly to upper level EB management in accordance with ISO 9000 and SEI CMM Frameworks. The Software Development Process, including the software assurance activity, is enforced through strict imposition of Configuration Management (CM). The CM tools used by EB include process management features to define developer roles. The tools also support development through formal CM in accordance with MIL-STD-973.

The Navy enhances software quality assurance via the Independent Verification and Validation (IV&V) team activities. IV&V provides management insight into process, progress, and product risk, and helps assure the system is ready for at-sea operations. The IV&V team assesses the technical and performance integrity of the software products being developed by the prime contractor. This activity ensures the software correctly performs its intended functions, the software does not perform any unintended functions, and the quality of the evolving software products remains high. During the initial SEAWOLF Class SCS development, IV&V played only a small role due to limited funding and scope. The Navy SCS IV&V Team played a much greater role early on in VIRGINIA's development phase than it did on the SEAWOLF Program. For VIRGINIA Class Ship Control System, the scope of the IV&V Team effort was established based on budgetary and risk tradeoff discussions with PMS450 management. The IV&V Team has a direct influence on the program decision and approval process.

The IV&V team provides technical reviews of prime contractor products for which the Navy is responsible to approve. This team is lead by civil servants from the NSWC Carderock Division, and includes individuals from NUWC experienced in development of software for complex weapons systems. By working as a partner in an IPT environment, IV&V team members are able to identify and resolve process non-conformances at the earliest stages where changes have the greatest improvement to software quality.

In addition to traditional IV&V review and audit activities, the team provides onsite review and approval of Problem Trouble Reports, witness and approval of requirements verification, and conduct of longevity and endurance testing of all major software releases prior to and including acceptance and installation. The IV&V team works closely with the system developer and uses existing software configuration management tools to conduct independent audits of software processes, safety, development, and test documentation. The team also provides oversight of informal and formal software testing and system level testing.

<u>Key Observations: Quality Assurance</u>

- The Lead Design Yard, General Dynamics Electric Boat Division conducts a separate and distinct software quality assurance activity using proven processes and improvements that leverage software quality assurance audits for both products and process.

- The Navy enhances software quality assurance via Independent Verification and Validation (IV&V) team activities.
- For VIRGINIA Class Ship Control System, the scope of the IV&V Team effort was established based on budgetary and risk tradeoff discussions with PMS450 management. The IV&V Team has a direct influence on the program decision and approval process.

Reviews (Navy)

The VIRGINIA Class Ship Control System was developed under the full suite of DoD-STD-2167A processes, milestones, and reviews. The software was designed and built in seven (7) Software Builds, each of which consisted of four phases - Planning, Software Development, Standalone CSCI Testing, and System Build Integration Phase. Milestones were tracked through each build phase and met defined entrance and exit criteria. Reviews were system, hardware or software in nature and included the System Requirements Review and the Preliminary Design Review. Later reviews also included a Critical Design Review (CDR). The CDR was broken into incremental Hardware and Software CDRs to accommodate the size and complexity of the system.

The fault-tolerant mechanisms in the Ship Control System represent a first-time fielding of a software based fault-tolerant scheme on COTS hardware. Fault-tolerant experts from industry, including Carnegie-Mellon University, University of Texas, and WW Technology, along with experts from the Naval Air Warfare Center (NAWC), were assembled to provide technical guidance with this part of the system and software development. During software detailed design, EB was encouraged to, and did, consult with the Navy's Software Program Managers Network (SPMN) for expert advice on software development. EB processes were modified to address the SPMN recommendations. One of the most valuable changes was to initiate formal peer reviews of the software requirements documents, design, and code products. The resulting code has shown quality significantly above that typical in such a complex system, as shown by the extremely small number of high priority software Program Trouble Reports (PTRs), the overall small amount of PTRs, and the significant success in software and system testing.

Key Observations: Reviews

- The VIRGINIA Class Ship Control System was developed under the full suite of DoD-STD-2167A processes, milestones, and reviews. Each milestone met defined entrance and exit criteria.
- The software was designed and built in seven (7) Software Builds, each of which consisted of four phases: Planning, Software Development, Standalone CSCI Testing, and System Build Integration Phase.
- The consistent use of formal peer reviews was a major contributor to software quality for the VIRGINIA Class.

Work Review Processes (Navy)

Formal software inspections are performed on the VIRGINIA Class Ship Control System software. The software leads and the *Continuus* process management software ensure that the inspection process is followed. The software inspections are done, for example, on new functional requirements identified late in the development that are deemed critical for initial system delivery. Metrics collected from the inspections are used to identify inspection process outliers. The outliers consist of units where too few defects were found or units where the defect density is too high. This data is used to determine if a unit should undergo additional inspections or, in cases with high defect densities, whether there is a systemic problem caused by a poor design or specification requirement.

Key Observations: Work Review Processes

- The Navy utilizes the *Continuus* process management software to ensure that software inspection processes are followed.

Audits (Navy)

The SUBSAFE concept of a functional audit has not been employed for Ship Control System software development. However, the Navy IV&V team has performed periodic audits of EB's software development folders to ensure the developer has followed their software development processes and procedures.

Incremental design verification was achieved by performing informal system integration and testing at each of the software builds. The Navy IV&V Team began an incremental Functional Configuration Audit to ensure system requirements were properly allocated and verified via testing. There are also the formal Functional Configuration Audits (FCA) and Physical Configuration Audits (PCA).

The FCA includes a review of all aspects of requirements traceability and verification of requirements fulfillment at each level including dockside and at-sea testing. Functional audits consist primarily in ensuring that requirements have all been implemented or accounted for in the system, and that supporting documentation is complete. An as-built analysis is done as well on both the software and hardware to ensure the functional requirements are met.

The system, including the software, underwent formal System Acceptance Testing on a shipset copy of the system hardware in the software development laboratory. The resulting final software was then delivered by replacement of memory boards from the system under test to the lead ship in the shipyard. The software PCA is essentially a verification that the executable software can be regenerated from source code and that the configuration delivered to the ship was the same as that tested in the lab.

In the case of the VIRGINIA Class Ship Control System, IV&V conducted the PCA/FCA. The contractor supports the PCA/FCA primarily by providing the necessary documentation and access to the system to complete the audits.

Key Observations: Audits

- The NAVY IV&V team has performed periodic audits of EB's software development folders to ensure the developer has followed their software development processes and procedures.
- Incremental design verification was achieved by performing incremental Functional Configuration Audits to ensure system requirements were properly allocated and verified via testing at each of the software builds.
- Functional Configuration Audits ensure that requirements have all been implemented or accounted for in the system and that supporting documentation is complete
- Physical Configuration Audits (PCAs) verify that the executable software can be regenerated from source code and that the configuration delivered to the ship is the same as that formally tested and accepted under laboratory conditions.

Control Boards (Navy)

Typically, several levels of Control Boards are utilized. At a system level, such as Ship Control, a SIT Configuration Control Board (CCB) is utilized for all changes within the Ship Control boundary. Above the SIT CCBs, there is a Non Propulsion Electronic System (NPES) CCB, which includes all the major subcontractors and government representatives. Lastly, there is a NAVSEA Government Board that reviews proposed changes to the submarine. Each of these boards is essentially a configuration management board. Important to the safety aspects of these reviews is the fact that the Cert PAT serves as a certification and oversight board independent of the program manager. Eventually, a process based around the *Requirements Manual for Submarine Fly-By-Wire Ship Control Systems* may supersede the Cert PAT approach for VIRGINIA.

Key Observations: Control Boards

- The Cert PAT serves as a certification and oversight board independent of the program manager.

Independent Assessment (Navy)

Several independent assessments of EB's software development processes were conducted during development of the VIRGINIA Ship Control System. Early in the Conceptual Design Phase, experts from Naval Air Systems Command and their support contractor assessed the fault-tolerant architecture. The architecture for this software was significantly modified based on the recommendations of this team. A team from the Commander, Operational Test and Evaluation Force (OPTEVFOR) assessed the overall software development process during preliminary design. A technical review of the design decision technical content and the process for selection of the internal Ship Control data bus architecture was conducted by a “Red Team” that included representatives from the Naval Undersea Warfare Center (NUWC), Lockheed-Martin Corporation, and AT&T Corporation.

OQE resulting from the safety analysis of the system and software must be provided to the Cert PAT. One item of OQE required by the Cert PAT was a review by the Software System Safety Technical Review Panel (SSSTRP) of the WSESRB. The WSESRB is the Navy’s premier weapons safety organization. The Cert PAT required that the SSTRP concur that the software-oriented safety analysis was appropriate to ensure maximum reasonable assurance that the VIRGINIA Class submarine Ship Control System will be safe to operate. EB provided detailed presentations on their software safety analysis process to the SSSTRP during preliminary design and during the safety analysis. In both cases, the SSSTRP provided concurrence that the software-oriented safety analysis was appropriate.

Key Observations: Independent Assessment

- Several independent assessments of EB’s software development processes were conducted during development of the VIRGINIA Ship Control System.
- Objective Quality Evidence (OQE) resulting from the safety analysis of the system and software must be provided to a Certification Process Action Team (Cert PAT).
- EB twice provided detailed presentations on their software safety analysis process to the Software Subcommittee System Safety Technical Review Panel (SSSTRP). In each case, the reviewing team provided a favorable report.

3.2.5 Certification Processes (Navy)

Certification Audits (Navy)

A ship certification audit for a software-driven system, as currently proposed, will have a process that parallels the process for ship SUBSAFE certification. The Cert PAT requires completion of the FCA and PCA as part of the overall safety certification for initial delivery. An audit will occur prior to float-off and prior to initial fast cruise (i.e., dockside sea trials simulation). An audit prior to completion of the Post-Shipyard Availability (a one-time availability conducted about a year after delivery) will occur on a ship-case basis. Thereafter, an audit will occur prior to completion of major industrial availabilities (major availabilities are defined as those having a duration of six months or longer).

Key Observations: Certification Audits

- A ship certification audit for a software-driven system, as currently proposed, will have a process that parallels the process for ship SUBSAFE certification.
- An audit will occur prior to float-off and prior to initial fast cruise, or dockside sea trials simulation.

Certification Review Process (Navy)

The Ship Control System software is tested in a laboratory environment on a tactical shipset of system hardware with simulated ship interfaces. This testing verifies that system functional requirements are met. Shipboard testing on the fielded system dockside and at-sea accomplishes certification of the system performance. The Cert PAT review represents the final certification review prior to the ship’s first at-sea tests, but is preceded with the FCA, PCA, and numerous Safety SIT status meetings. The Cert PAT output is then input to the overall ship certification authorizing sea trials. However, until hydrodynamic and ship control trials are completed, certification for full and unrestricted operation is withheld.

Key Observations: Certification Processes

- The Cert PAT requires completion of the FCA and PCA as part of the overall safety certification for initial delivery.
- The Ship Control System software is tested in a laboratory environment on a tactical shipset of system hardware with simulated ship interfaces in order to verify that system functional requirements are met.
- Shipboard testing on the fielded system dockside and at-sea accomplishes certification of the system performance. The Cert PAT review represents the final certification review prior to the ship’s first at-sea tests.

3.3 Comparative Context & Opportunities

3.3.1 Comparative Context

The Navy's submarine and NASA’s human space flight programs have a number of factors in common, the most important of which is a dedication and commitment to safety while conducting missions of national importance in very hostile and hazardous environments. However, significant differences (e.g., managerial, organizational, and cultural) also exist. In order to provide a proper contextual background against which the key observations and opportunities developed from this software benchmarking exchange can be appropriately evaluated, the following paragraphs address some of the overriding issues in NASA’s and the Navy’s software programs.

Integration of Contractor and Civil Servant Personnel

NASA’s Space Shuttle project development teams, with highly integrated mixtures of NASA and USA (Boeing, Lockheed-Martin) personnel all working side-by-side, produce a single, integrated software product. While recent NAVSEA developments have included very close relationships between the Navy and the Prime Contractor, such intermixing of personnel is not typical.

NAVSEA’s fly-by-wire submarine Ship Control System developments have each been accomplished with a contractor Lead Design Yard while a Navy laboratory provides automatic control algorithms. With the VIRGINIA Class Ship Control System, the Navy has become quite stringent in ensuring the Lead Design Yard follow appropriate software development practices. Formally documenting these practices is the norm.

Requirements for the Navy laboratories, however, have typically been much less stringent and the Lead Design Yard has little insight into the Navy product until it is nearly complete. This process has the potential to cause software integration problems and raise questions about the consistency of the development and safety analysis processes used by each activity.

Technical Authority for Software Development Standards

Technical authority for NASA software development has historically resided with the program or project manager. Software Assurance and the IV&V Facility generally serve in advisory roles, with an independent reporting chain to appeal directly to Headquarters OSMA. NASA is in the process of changing this policy, and is preparing to require that all software projects Agency-wide adhere to a Software Assurance Standard and Software Safety Standard, both of which have been recently updated by Headquarters OSMA. This policy would require a formal “deviation” if it is anticipated that a standard would not be met. If a project is already underway and it is determined “after the fact” that a requirement will not be met, then a formal “deviation” is required.

Technical authority for NAVSEA hardware and software systems lies solely with the Chief Engineer, NAVSEA 05. Technical authority for software development, however, is organized by system, (e.g., the ship control system), and NAVSEA 05 leaves software development up to the system technical expert and the program manager.

While NASA has identified considerable room for improvement by more consistent and forceful imposition of NASA software development standards, NAVSEA does not maintain any centralized standards. Rather, the imposed standard is left to the discretion of each system technical expert or program manager. As a result, NAVSEA's process lends itself to being "hero driven." This is the lowest form of software development and one that should be avoided to reduce schedule and cost risk. Additionally, the Navy lacks detailed agency level guidance on the amount, nature, and focus of IV&V for software. Despite a centralized technical authority, each ship control system development in the past decade (SEAWOLF, VIRGINIA and ASDS) has approached IV&V somewhat differently.

3.3.2 Opportunities

Notwithstanding the issues cited in section 3.3.1, there are potential opportunities for improvement and enhancement that NASA and the Navy may wish to consider as they seek to continuously improve the safety of their software programs.

3.3.2.1 Opportunities – NASA

As a result of NASA's effort to prepare for meetings with the Navy, the following areas for improvement were identified by NASA SA personnel.

Opportunity #1: Reappraise Shuttle software using CMM or CMMI.

NASA may want to consider reappraising Shuttle on both the contractor and civil servant sides using CMM or CMMI to verify that their exemplary rigor has not diminished. This is especially important since the Shuttle is still certified at CMM Level 5 despite not having been appraised in 8 years, during which time it has changed contractors twice.

Opportunity #2: Strengthen the levels of defense for assuring software safety

NASA may want to consider strengthening its levels of defense for assuring software safety and quality. Specifically, this opportunity includes establishing and implementing better contractor requirements (Level 1), bolstering the Agency's Software Assurance (SA) resource pool (Level 2), and ensuring that IV&V is called upon only in critical situations (Level 3).

Establishing better contractor requirements involves both creating standards for consistent contract content with clear, identifiable deliverables and allowing greater recourse for holding the contractors accountable for meeting their contractual requirements.

Bolstering the Agency's SA resource pool involves several steps. First, the group needs to define a clear and appealing career path for bright young talent. Next, it would need to implement training to help current employees improve their skills. Finally, top down recognition and assistance would promote awareness about these changes and influence the culture change needed to make the Software Assurance role more visible in the NASA community. NASA has already started to create a consistent, professional approach to Software Assurance via the two standards, NASA-STD-8739.8, NASA Software Assurance Standard, and NASA-STD-8719.13, NASA Software Safety Standard.

Finally, IV&V is frequently called upon as part of normal operations instead of only in critical situations, as is its charter. The group, therefore, can be overloaded, inhibiting its ability to perform at the high standards of which it is capable. By bolstering the Agency's SA resource pool, NASA has the opportunity to reverse the trend of IV&V performing the second, rather than the third, line of defense for which it was intended. Reinstituting SA's role as the second line of defense would enable IV&V to focus on performing at a high level of quality in the critical situations for which it is designed.

Opportunity #3: Strengthen Agency CMM/CMMI related requirements for mission critical software**.**

When updating NPD 2820, NASA Software Polices, NASA may want to consider not only keeping, but potentially strengthening, the CMM/CMMI related requirements for organizations developing or maintaining mission critical software. Some of this work has already been initiated in NASA SWE NPR 7150.2 (Software Engineering Requirements), which was in the administrative review cycle at the time of this report.

Opportunity #4: Institute software inspection efforts Agency-wide.

The use of rigorous formal software inspections, developed based on industry best practices such as those prescribed by Fagan and Gilb, has provided positive lessons learned for NASA. NASA is considering instituting an Agency-wide effort to re-infuse these, or similar inspection processes, into all software intensive projects.

3.3.2.2 Opportunities – Navy

Opportunity #1: Develop a centralized NAVSEA software IV&V organization

As a long-term goal, NAVSEA may want to consider developing a centralized IV&V organization similar to NASA's approach. This organization would be responsible for setting technical standards for software IV&V, including project assessments, IV&V approach, and magnitude of the effort. Such an organization would be an integral member of each NAVSEA project team and would participate in each major program review. Assessments and recommendations would be provided both to the applicable PEO and the Program Manager. The Program Manager would then be responsible to the PEO to accept the recommended approach or provide technical rationale for not doing so. By implementing an independent organization with responsibilities mandated at the highest levels of NAVSEA, conflicts with programmatic constraints (cost) can be forced up front to ensure an appropriate level of software IV&V is applied to support overall program safety and quality assurance requirements. In the short-term, NAVSEA may want to establish IV&V assessment guidance similar to that developed by the NASA IV&V Facility.

Focused discussions with NASA IV&V personnel at the Fairmont, WV facility should be considered to discuss topics such as return on investment, objective criteria for choosing the extent and nature of IV&V for a specific project, reporting requirements, independent testing requirements, and the relationship of IV&V activities to software safety analyses.

Opportunity #2: Formalize Software Development as a Recognized and Warranted Technical Discipline at NAVSEA Headquarters.

NAVSEA may want to consider developing a warrant holder for software development, including quality assurance and software safety. The warrant holder and his/her organization would be responsible for setting technical standards for software development across NAVSEA PEOs. As with the NASA approach, individual projects would be permitted to use industry (contractor) or other DoD standards as long as the Program Manager can demonstrate the selected standards meet or exceed the NAVSEA standard. By establishing a NAVSEA centralized standard for software development, individual programs would be forced to develop and budget for appropriate software development activities from the program inception. Likewise, the nature and quality of design deliverables that support software certification would be established early in the program with buy-in from the appropriate certifying authority, thereby preventing surprises late in the program.

Opportunity #3: Revise and Implement NAVSEA-wide Software Standards

NAVSEA may want to consider closely following NASA's efforts to revise their software development and safety policies, and NASA's efforts to implement these as NASA-wide standards. The technical content of these documents and the administrative approach used to impose them on NASA programs may provide valuable lessons learned for a new NAVSEA software development warrant holder trying to standardize software development at NAVSEA.

Opportunity #4: Integrate Navy Laboratory Software Development into Lead Design Yard Efforts

NAVSEA may want to consider fully integrating the Navy laboratory software development efforts into the Lead Design Yard efforts to ensure a seamless product delivery. NASA's highly integrated project teams, with NASA and USA personnel all working side-by-side, produce a single integrated software product. NAVSEA's fly-by-wire submarine ship control system developments have each been accomplished with a contractor Lead Design Yard and a Navy Laboratory that provides automatic control algorithms working independently of each other and communicating infrequently until the end of the process. This process has the potential to lead to significant software integration problems and raise questions about the consistency of the development and safety analysis processes used by each activity.

The Program Manager could reduce these concerns and lower his/her risk by fully integrating the Navy laboratory software development efforts into the Lead Design Yard efforts, including meeting all the software development standards imposed on the Lead Design Yard by the Program Manager. Initial development costs might rise, but long-term lifecycle costs and risk would be reduced, safety would be enhanced, and potential software integration schedule impacts could be avoided.

Opportunity #5: Perform Formal Causal Analysis on Software Deficiency Reports

NAVSEA may want to consider adding a formal requirement to do a causal analysis on software deficiency reports throughout the life cycle. While software deficiency reports are evaluated and corrected as appropriate to their severity, causal analysis is not currently a formal activity. Formally requiring this analysis would help ensure that critical problems are corrected throughout the software at their first detection. It could also provide lessons learned for later software developments.

Opportunity #6: Review NASA's SLEP Program for Lessons Learned on Software Reuse

NAVSEA may want to consider closely reviewing NASA's former Shuttle Life Extension Program (SLEP) for lessons learned in software reuse, modification, and recoding. Fly-by-wire ship control systems on Navy submarines have only been fielded for a few years, but hardware and software technology obsolescence is already occurring on fielded and even yet-to-be fielded systems. The Navy may be able to gain valuable insights on this problem by understanding and following NASA's decision making processes applied to similar problems encountered in the SLEP.

The Launch Processing System (LPS) at KSC decided against a full-blown re-design to address hardware obsolescence and instead went into a "survivability" mode in order to stretch additional life out of the system, despite its safety critical nature. The Navy faces obsolescence questions on a daily basis for both delivered and new construction submarines. In particular, lessons learned from NASA SLEP may have direct applicability to future SEAWOLF Class Ship Control Processing Unit (SCPU) life extension/replacement since the two programs use similar custom design hardware.

Further discussion on decision criteria for re-design, "survivability" mode, or system abandonment could benefit both NASA and the Navy by leading to more consistent decision making.

Opportunity #7: Pursue NASA Software Assurance Audit and Independent Assessment Lessons Learned

NAVSEA may want to consider targeted discussion with NASA on their Functional & Program Compliance Verification Audits and Independent Assessments (IAs). If NAVSEA develops a warrant holder for software development and charges that person with setting standards for software development of NAVSEA systems, it will be necessary for NAVSEA to ensure that these processes are being followed. NASA's Functional & Program Compliance Verification Audits and Independent Assessments can likely provide many lessons learned in achieving this assurance.

Opportunity #8: Exchange NASA/Navy COTS Hardware/Software Information and Certification Processes

The International Space Station (ISS) program is heavily dependent upon commercial off-the-shelf (COTS) electronics and software. With the move to COTS on the VIRGINIA Class Submarine Ship Control System (SCS), NAVSEA may want to consider holding targeted meetings with NASA ISS personnel to discuss issues related to COTS. Such issues include but are not limited to hardware and software quality assurance, safety analysis in the absence of or with limited design data, technology obsolescence and refresh, unused ("dead") code, and configuration control. Since the Navy has moved to COTS for submarine sonar systems, it may be appropriate to bring those Navy activities working the Acoustic Rapid COTS Insertion (ARCI) program into the discussion.

Furthermore, NAVSEA is currently finalizing a program for achieving and maintaining hardware, software, and system certification of the VIRGINIA Class Submarine. Certification of the first, true fly-by-wire submarine ship control system on the SEAWOLF Class was accomplished in a hero driven, ad-hoc fashion. Despite attempts to avoid that on the VIRGINIA Class, only recently has the Navy been able to begin to document and formalize the process, products, and procedures needed to achieve and maintain this certification in the COTS-intensive environment of the VIRGINIA Class SCS. Initial certification of VIRGINIA Class SCS (774) was to the FBW SCS manual with Cert PAT acting in a similar role as for previous SEAWOLF SCS certification but with additional OQE requirements driven by the manual. Future certification will be totally under the organization established by the manual. As this process is finalized and initial certification achieved for the VIRGINIA Class SCS, NAVSEA should share the process and sample products with NASA for potential use in ISS and future shuttle upgrades.

Opportunity #9: Consider a Test-oriented Design Language Similar to NASA's *GOALS*

NASA's custom built, test-oriented design language, *GOALS*, assists engineers in writing their own test programs. This may be worth further investigation by the Navy for cost and schedule savings if it can be ensured that the loss of independence (developer v. tester) does not compromise the process.

Opportunity #10: Consider Alternative Selection Criteria for SW Vendors

NAVSEA may want to consider requiring CMM, and perhaps CMMI, as a selection criteria for software vendors.

APPENDICES

Appendix A: Software Subgroup Report I – Key Observations

Appendix B: Elements of Safety Critical Decision Making Initiative Plan

Appendix C: NNBE Memoranda of Agreement (MOAs)

Appendix D: Navy Memos outlining Software Safety Criteria

This page intentionally blank.

APPENDIX A: Software Subgroup Report I – Key Observations

Appendix A-1: NASA – Summary of Key Observations

Summary of Key Observations – NASA	
3.1.1	**Organization – NASA**
	- NASA's organization is divided into programmatic and functional offices. Both participate in SMA processes and policies. - The OSMA is the functional office specifically charged with overseeing SMA for NASA, which includes software. It is divided into Headquarters and Center level organizations. SA is addressed as a function of overall SMA, while IV&V is treated as an independent software SMA organization within the office. - Each Enterprise within NASA is charged with adopting SMA processes for a particular program or project. Software SMA on a programmatic level is typically governed by control boards and review panels. - The project or program managers (PMs) have historically been the technical authority for their individual NASA projects. - The project or program manager is required to create a software plan for a project that is compliant with NASA's Software Assurance and Software Safety standards. - Center SA and IV&V perform advisory roles on projects, in proportion to software criticality. They also serve as an independent reporting authority for safety issues. - While the PM is ultimately responsible for safety, both SA and IV&V have the capability to appeal an issue all the way to OSMA for arbitration, if they feel a safety concern has not been adequately addressed on a program. - Each project reports its risk management plan, status, budget, and schedule to the GPMC or the PMC. - NASA has applied a form of performance-based contracting to many new projects and programs, including software implementations. - NASA has developed a highly integrated approach to contractor management, where civil servants work in the same physical location as contractors, often sharing tasks and corroborating on software development. - The link between civil servant and contractor is essential for NASA to manage its projects and programs, and it also serves to minimize the cost of requirements definition for future projects.

Summary of Key Observations – NASA

3.1.2 Software Safety Requirements – NASA

- NASA assumes that software can always fail, despite best efforts to ensure safety, reliability, quality, and maintainability.
- True software safety requires building safety into the system throughout the development life cycle, rather than adding safety as an afterthought.
- While software deficiencies are addressed as they are discovered, unmitigated hazards are traced back to their root causes and considered a result of flawed requirements or a flawed safety process. NASA believes safe, high-quality software is a byproduct of continually updated, refined, and validated software SMA processes. By fixing processes rather than just problem occurrences, future problem occurrences are reduced.
- The Software Safety Standard and Software Assurance Standard are the overarching requirements documents for software SMA. In most cases, these documents closely follow industry standard processes and comply with IEEE standards; however, both are specifically tailored to NASA.
- While there are NASA guidebooks for software safety, how these functions are carried out is at the discretion of the program manager or found in Center-specific and program-specific standards or processes.
- The project or program manager has historically owned project-specific SW requirements. Software Assurance personnel track a project's requirements and their adherence to the overarching Software Assurance Standard and Software Safety Standard.
- Specific software SMA requirements are often created at the program or project level, but all such requirements must be compliant with the governing Software Safety Standard and Software Assurance Standard.

3.1.3 Implementation Processes – NASA

- Software safety has been considered at earlier points in the tool development life cycle, thus allowing earlier proactive reduction of safety errors.
- Software SMA Requirements depend on the nature of the project. In NASA's revised Software Safety Standard, all projects will undergo a hazard severity and safety analysis in order to determine the appropriate level of software SMA applied throughout the life cycle of the project.
- SW Safety "litmus" test criteria are used to identify safety critical software.
- Software safety has been considered at earlier points in the tool development life cycle, thus allowing earlier proactive reduction of safety errors.
- Based on the *Software Safety Litmus Test*, the designation of a new software project as safety-critical during the concept development phase will help ensure software safety is considered correctly in each step of the project life cycle.
- NASA rarely makes use of scheduled upgrades for maintenance and upgrades

of COTS software because it can be very expensive and require extensive testing. Instead, NASA has tried to minimize by using older and more established versions of its own software for as long as possible.

- NASA tracks software deficiency reports and performs formal causal analysis to determine the root cause of software defects.
- NASA has accepted the Software Engineering Institute Software Capability Maturity Model and CMM-Integrated processes as key elements in achieving some of NASA’s goals.
- Despite changes in NASA’s contracting organizations for Shuttle flight software, the rigorous procedures and processes have been adopted across contractors.
- An Agency-wide software improvement initiative, begun in 2001, relies heavily on CMM/CMMI.
- The Space Shuttle Program has an extensive training regimen for software systems that includes classes, simulations, and certification of qualified employees.
- NASA places a strong emphasis on mentoring and on-the-job-training as part of its training program due to the uniqueness and complexity of its systems and associated software.
- For the Space Shuttle, technology insertion / modernization projects are formed separately from the rest of Shuttle flight software and are run as a separate, phased projects up until final integration into the current Shuttle systems.
- All Shuttle technology insertion / modernization requirements are extensively reviewed by the Shuttle flight software and systems experts, the crew, Mission Operations, and Center SMA from both the contractor and NASA sides of the program.
- The use of the Shuttle Avionics Integration Laboratory (SAIL), which functions as NASA’s fourth Shuttle for the purposes of software testing, is crucial in testing all changes to the Shuttle software and crew interfaces.

3.1.4 Compliance Verification Processes – NASA

- Design verification for the Space Shuttle is achieved primarily through peer reviews and formal reviews from technical experts following structured processes and using consistent and thorough review checklists.
- Change control boards authorize changes and participate in formal reviews. These boards have both NASA and contractor representation, but changes must be approved ultimately by a NASA manager.
- Shuttle Flight Software has a very strong software inspection process that has been maintained for more than two decades. Out-of-tolerance indicators can catch problems early, keeping them from propagating into later quality gates (testing, etc.) where their probability of escaping into operations is higher.

Summary of Key Observations – NASA

	- There is a need to perform more regular audits of contractor and NASA Software Engineering by NASA SMA organizations. - Software control boards are an important aspect of managing software risks at the programmatic level and verifying software requirements implementation and compliance. - Software control boards are project-specific and report directly to the program manager or to parent control boards. - IV&V Independent Assessments (IAs) are used to identify where a program/project’s software may be weak and need additional analyses, processes, or verification. - IAs can be performed at the program, project, Center, and Agency levels. The newly created NASA Engineering and Safety Center (NESC) is also performing independent analyses and assessments on NASA programs.
3.1.5	**Certification Processes – NASA**
	- Software Assurance (SA) consists of the disciplines of software quality, software reliability, software safety, software verification and validation, and independent verification and validation. - The SA process is the planned and systematic set of activities that ensure conformance of software life cycle processes and products to requirements, standards, and procedures. - SA disciplines can be thought of as an umbrella risk mitigation strategy for ensuring that a system is both safe and of the highest quality possible. - The Shuttle Avionics Integration Lab (SAIL) represents the final set of system testing before software is certified for flight, and has identified errors which could have resulted in a hazardous situation during a shuttle mission.

Appendix A-2: Navy – Summary of Key Observations

Summary of Key Observations – Navy	
3.2.1	**Organization – Navy**
	- Software development at NAVSEA is conducted as an integral part of system development. The Program Office responsible for platform or system acquisition is also responsible for software acquisition for that platform and/or system. - Development of each subsystem/component is conducted in an integrated fashion with both hardware and software managed by a single System Integration Team. - Software and hardware development are not recognized as formal and distinct disciplines; instead, the NAVSEA technical authority for software and hardware development is rolled into the technical authority as organized by each major ship system. - Technical warrant holders are recognized experts in their fields and are empowered to make technical decisions for NAVSEA in their warranted field. As such, warrant holders are personally accountable to the Chief Engineer (NAVSEA 05) for technical matters regarding systems in their charge. - Although warrant holders currently do not exist for disciplines such as software development or software safety, development of the *Requirements Manual for Submarine Fly-By-Wire Ship Control Systems* may result in establishment of these warrant holders. - Software is provided as an integral part of developed or delivered ship systems. The Program Office is responsible for ensuring a sufficient budget for software development and software safety. The Program Office responsibility for software procurement follows ship system development and procurement. - Having the same technical and quality assurance personnel who supported the acquisition program office also support the in-service and disposition program offices provides continuity and benefits software maintenance and software safety. - The Integrated Product and Process Development (IPPD) contract approach benefits software development and software safety associated with the ship systems. Establishing combined government and contractor design/build teams promotes effective communications and ensures optimum decisions for product design/construction, risk management, and risk mitigation.
3.2.2	**Software Safety Requirements – Navy**
	- No formal NAVSEA institutional doctrine on software safety yet exists, but the safety philosophy ingrained in the submarine community carries over to software systems. - The recently adopted *Requirements Manual for Submarine Fly-By-Wire Ship Control Systems* institutionalizes a process-driven philosophy. - Software safety criteria identified by the Cert PAT define assertions that the system software must not do in order to be considered safe within the defined submerged operating envelope. - Key principles for successful software development include managed turnover, no

secrets, empowered individuals, earned value, metrics, and IV&V.

- New design software development is governed by the DoD 5000 series of documents that identify mandatory and preferred processes for defense systems acquisition. DoD 5000 currently recommends allowing the contractor to use their own best practice for software development upon approval of the Navy.
- The Program Office, Technical Authority, and lead design yard (EB) unanimously agreed to implement the VIRGINIA Class Ship Control System under the DoD-STD-2167 process.
- During the system development, significant tailoring was done to the safety analysis requirements document, MIL-STD-882C, in order to focus the analysis on software and ensure that specific identified hazards did not exist.
- The Ship Spec identifies the requirement for a ship safety program with new or significantly modified systems for a safety analysis per MIL-STD-882.
- A Certification Process Action Team (Cert PAT) identified software safety criteria for evaluation of the VIRGINIA Class Ship Control System. The associated system safety analysis was significantly modified to focus on these criteria while still retaining the basic MIL-STD-882 approach.
- The *Requirements Manual for Submarine Fly-By-Wire Ship Control Systems* may supersede the need for the Cert PAT to address Ship Control Systems.
- System specific requirements are first identified at the Ship Spec level and are then flowed down and imposed on the contractor throughout the system design documentation.
- The NAVSEA technical authority is the "owner" of the platform and system functional requirements for new design systems, including the software associated with those systems.
- Software safety criteria are imposed on the contractor by the technical authority via a formal process with concurrence of the Program Office.

3.2.3 Implementation Processes – Navy

- Concept development for the VIRGINIA Class Submarine Ship Control System was accomplished at the system level and centered around functional requirements and not specified safety requirements.
- Early during the concept development phase of the VIRGINIA Class submarine Ship Control System, a modular software design approach was used extensively to contain anticipated hardware/software changes and address concerns about obsolescence.
- A MIL-STD-882 system safety analysis was begun in the early stages of the VIRGINIA Class Ship Control System development. The software safety criteria, the MIL-STD-882 analysis, developed by the Cert PAT, was modified during detailed design to focus on software-oriented analysis.
- Unmet verification requirements are documented as deficiencies, resulting in a must-fix problem trouble report.
- The Ship Control Project utilized real-time structured analysis techniques for requirement development, included a design approach that emphasizes the critical SW design and performance threads, implemented software configuration

management and control processes, and employed software tools for developing unit test cases, documenting results, and analyzing test coverage.

- PMS450 has an active risk management program for all program risks, including software. As required by the VIRGINIA Class Risk Management Plan, one or more mitigation plans were identified for each risk.
- Each system or functional area has a Risk Area Manager (RAM) responsible for identifying risks and mitigation strategies, which are documented in a central risk database and tracked by the program’s risk manager.
- The EB development team implemented the Navy-accepted *Practical Software Measurement* approach to reduce risk by identifying program and technical issues, and selecting specific quantifiable measures to track the status and progress of issues.
- Development of each subsystem/component is conducted in an integrated fashion with both hardware and software managed by a single System Integration Team.
- Virginia Class Software IV&V has been conducted by the Navy as part of the SIT process in an Integrated Process and Product Team environment. The Navy was team-led by NSWC and included NUWC and contractor personnel.
- Tasking of System (SW/HW) supporting tasks to EB, Navy field activities, and directly supporting contractors is done annually by the Program Office via Individual Task Management Plans (ITMPs).
- Because of the safety-of-ship critical nature of the Ship Control System, a Safety Integrated Product Team (IPT) was established and charged with specific responsibility to ensure the safety analysis was properly conducted.
- Metrics collected from the inspections process are used to identify inspection process outliers. This data is used to determine if a unit should undergo additional inspections, or if there is a systemic problem.

3.2.4 Compliance Verification Processes – Navy

- The Lead Design Yard, General Dynamics Electric Boat Division conducts a separate and distinct software quality assurance activity using proven processes and improvements that leverage software quality assurance audits for both products and process.
- The Navy enhances software quality assurance via Independent Verification and Validation (IV&V) team activities.
- For VIRGINIA Class Ship Control System, the scope of the IV&V Team effort was established based on budgetary and risk tradeoff discussions with PMS450 management. The IV&V Team has a direct influence on the program decision and approval process.
- The VIRGINIA Class Ship Control System was developed under the full suite of DoD-STD-2167A processes, milestones, and reviews. Each milestone met defined entrance and exit criteria.
- The software was designed and built in seven (7) Software Builds, each of which consisted of four phases: Planning, Software Development, Standalone CSCI Testing, and System Build Integration Phase.
- The consistent use of formal peer reviews was a major contributor to software

Summary of Key Observations – Navy

quality for the VIRGINIA Class.

- The Navy utilizes the *Continuus* process management software to ensure that software inspection processes are followed.
- The NAVY IV&V team has performed periodic audits of EB's software development folders to ensure the developer has followed their software development processes and procedures.
- Incremental design verification was achieved by performing incremental Functional Configuration Audits to ensure system requirements were properly allocated and verified via testing at each of the software builds.
- Functional Configuration Audits ensure that requirements have all been implemented or accounted for in the system and that supporting documentation is complete
- Physical Configuration Audits (PCAs) verify that the executable software can be regenerated from source code and that the configuration delivered to the ship is the same as that formally tested and accepted under laboratory conditions.
- The Cert PAT serves as a certification and oversight board independent of the program manager.
- Several independent assessments of EB's software development processes were conducted during development of the VIRGINIA Ship Control System.
- Objective Quality Evidence (OQE) resulting from the safety analysis of the system and software must be provided to a Certification Process Action Team (Cert PAT).
- EB twice provided detailed presentations on their software safety analysis process to the Software Subcommittee System Safety Technical Review Panel (SSSTRP). In each case, the reviewing team provided a favorable report.

3.2.5 Certification Processes – Navy

- A ship certification audit for a software-driven system, as currently proposed, will have a process that parallels the process for ship SUBSAFE certification.
- An audit will occur prior to float-off and prior to initial fast cruise, or dockside sea trials simulation.
- The Cert PAT requires completion of the FCA and PCA as part of the overall safety certification for initial delivery.
- The Ship Control System software is tested in a laboratory environment on a tactical shipset of system hardware with simulated ship interfaces in order to verify that system functional requirements are met.
- Shipboard testing on the fielded system dockside and at-sea accomplishes certification of the system performance. The Cert PAT review represents the final certification review prior to the ship's first at-sea tests.

APPENDIX B: Elements of Safety Critical Decision Making Initiative Plan

Changing NASA's Decision-Making Culture

Issue:

Results from the NASA/Navy Benchmarking effort and the Columbia Accident Investigation Board have indicated that improvement in NASA's critical decision-making is necessary.

Response:

The Safety Critical Decision-Making (SCDM) Training Initiative will involve senior-level participation and motivation combined with facilitated sessions. The process will be championed at each Center by a senior staff member(s) and will include a communication and measurement program. The initial training components will be combined with annual refresher sessions which will identify and stress an evolving decision-making culture.

The Academy for Program and Project Leadership (APPL) will serve as an overall coordinator for the development and facilitation of management and program/project workshops, ensuring consistency in the method of delivery and message. The APPL Director, Dr. Edward Hoffman, will work with the appropriate Headquarters Departments and Center staffs to administer the SCDM Training Initiative, with the APPL Deputy Director, Tony Maturo, leading the procurement activity.

Overview:

The Administrator has clearly and forcefully made the point to the public and the Congress as well as the entire NASA workforce, including contractors, that a culture change is necessary and crucial to the future of the Agency. Executive leadership must continually communicate the reasons for the culture change, articulate a new vision, and describe the first steps toward making the new vision a reality. This cultural change must emphasize:

- Alignment and allocation of appropriate and adequate resources,
- Implementation of organizational and/or process changes within the Agency to support, enable, and sustain the desired behaviors,
- Realistic expectations and accountability for realistic results,
- Clear and consistent communications about the importance of the initiative and the progress made,
- Rewards and recognition for those exhibiting the desired behavior, and
- Holding accountable those who impede the desired behavior.

Elements of Cultural Change:

- Training to spread a common understanding of the decision-making issues that can lead to project success/failure and the techniques to deal effectively with those issues;
- Implementation of a common vocabulary to improve communications among various echelons of the Agency management structure;
- Adherence to an accepted code of conduct that explicitly defines expected communication and decision-making protocols based on project opportunity and risk.

It will be incumbent upon each Center's leadership to enforce the accepted code of conduct to prevent what some have described as a "culture of fear" from impeding mission success.

Seminars and Workshops:

Led by the active participation of NASA senior leadership, the APPL-developed workshops will engage NASA leaders across the Agency in a frank dialog about present NASA decision-making processes and how they can improve NASA's ability to make collaborative decisions under conditions of conflict, ambiguity, and uncertainty. These facilitated seminars and workshops will assist the NASA workforce in examining their individual and collective roles in safety-critical decision-making processes, and will address decision-making in each phase of the program/project life-cycle from initial requirements definition through operation and subsequent retirement of the system. Seminar and workshop content, structure, and functionality will remain dynamic and will be modified and updated, as appropriate.

Seminar and Workshop Implementation:

Training initiative content and focus are designed to address specific decision-making needs and issues at four levels: 1) all NASA employees, 2) Senior Leadership, 3) Senior Management, and 4) Program/Project team members, including on-site contractors, as appropriate. In general, workshops will require participants to operate outside of their established comfort zones. Content will be compelling and highly interactive, and will provide practical decision-making process knowledge directly applicable to participant roles and responsibilities.

The workshops will include high-impact videos, case studies, and role-playing scenarios. Specific training elements include:

- Inviting nationally recognized organizational behavior and decision making experts to participate in the workshops.
- Using professional-quality multi-media presentations
    - Video-taped presentations from nationally-renowned decision-making experts
    - Training videos showing reenactments of scenes such as the preflight Challenger meetings
- Reviewing case studies that highlight decision making processes for highly-complex, tightly-coupled organizations and systems. These case studies will include examples both internal (e.g., Columbia, Challenger, Mars Polar Lander, etc.) and external (Petrobras, Chernobyl, USS Bonefish) to NASA.

- Conducting group activities/role-playing designed to simulate high-pressure decision environments.
- Providing each workshop participant with appropriate text materials (one or two main books) as a personal resource and providing a larger set of decision-making books for each Center's library.
- Requiring each participant to develop personal action plans for improvement in decision-making areas. These must be discussed with supervisor during annual reviews.

Measuring Cultural Change:

Training alone will not result in the desired change in behavior and culture. Given the objective to change NASA's safety decision-making culture, we must define direct measures of the initiative's results, develop an annual assessment questionnaire based on these measures, and survey alumni of the program to evaluate improvement against the current baseline. In addition, an annual questionnaire will be completed by all employees to compare with the alumni self-assessments to obtain the agency perception of degree of cultural change actually occurring in such areas as minority opinion acceptance, proper communications, and use of lessons learned.

Pre- and post-workshop focus groups, lasting one to two hours each, will be established to identify key indicators tied to NASA's decision-making abilities. Focus group participants will be selected based on Enterprise and Center recommendations. Once baseline measures are established, NASA leaders can determine what additional interventions are necessary or whether the workshops should be repeated periodically (e.g., during new employee indoctrination, mandatory for new project team startups, etc.), based on their effectiveness in helping to improve collaborative decision-making across the Agency.

Outlines of Training Elements:

Appendices B-1 through B-4 provide outlines of the four core elements of the Safety Critical Decision Making Training initiative.

This page intentionally blank.

Appendix B-1: Agency All-Hands

(1-hour Session)

This brief session will set the stage for the SCDM Initiative, establish the support from the Senior Leadership levels, and encourage participation from all employees. It will link the initiative to the need for cultural change while retaining the impressive strengths of the agency and invoke a requirement for encouraging and using minority opinions.

Agency All-Hands Outline

Time	One Hour Session
1 hour	Administrator Introduction
	Review NASA's heritage of accomplishments
	Recognize that Columbia incident highlighted some problems in Agency, e.g., CAIB recommendations
	Discuss NASA's on-going responses to these problems (e.g., decision-making training and other cultural initiatives)
	Establish the importance of this process and of attending the workshops
	Provide a vision of how the agency ought to work more effectively: • Group dynamics and team decision-making processes • Organizational roles and responsibilities • Communication/information flow/dissenting opinions
	Assure that senior management will support any employee bringing concerns to superiors or to designated safety officers
	Express confidence that NASA human-rated space flight programs will successfully accomplish the changes required and has a bright future ahead

This page intentionally blank.

Appendix B-2: Senior Leadership Seminar

(Half-day Session)

The major focus of the seminar is to benchmark and improve the critical decision-making skills within NASA, with a longer-term goal of changing the decision-making culture Agency-wide. Topics will include: critical decision-making strategies, risk assessment, NASA safety culture (including socio/psychological group dynamics and influences), and individual accountability within the system at NASA. Training methods used through the four-hour session will include lecture and facilitated group discussion.

Senior Leadership Seminar Outline

Time	Half Day Session
1:00 p.m.	Current NASA Decision-Making Culture - Reality Check *Knowledge Café: answer the following questions (40 minutes)* • *How are critical decisions made in your organization?* • *Describe the overall communication environment, including flow of critical information to decision-makers.* • *What is your organization's attitude towards voicing minority opinions or concerns?* • *How is risk assessed and/or managed?* B. Reconvene As One Group - Identify Patterns and discuss (20 minutes)
2:00 p.m.	Challenger Discussion *View Challenger Video (15 minutes)* *Facilitated Discussion of the Challenger Decision Process (30 minutes)*
	BREAK (15 minutes)
3:00 p.m.	Decision-Making Model *Framing and Risk* *Generating Alternatives* *Decision-making techniques* • *Rational vs. Intuitive processes*
4:00 p.m.	Dynamics of Groups Characteristics of group decision-making *Divergence/convergence, Collaboration* *Decision Traps and Cognitive Biases* • *Group Think* • *Anchoring* • *Confirming Evidence* • *Status Quo*
4:45 p.m.	Wrap Up: Give course evaluation
5:00 p.m.	ADJOURN

Senior Leadership Seminar – Focus Areas

Area	Action
Agency Culture	• Examine NASA, Enterprise, Center, and Program decision-making cultures. Identify recurring themes and patterns. • Review NASA's process for escalating safety concerns. • Identify techniques for developing, considering, and incorporating minority dissenting opinions. • Discuss relationships with contractors and how to evaluate accuracy of their decisions and program inputs • Analyze paths of information flow to decision-makers; define ways to improve accuracy and comprehensiveness.
Group Dynamics	• Examine models of group dynamics and collaborative decision-making, including socio/psychological components and "groupthink." • Participate in group-based learning scenarios, demonstrating collaborative decision-making techniques.
Decision-making Techniques and Strategies	• Understand and apply simple decision-making techniques. • Discuss the differences between analytical and intuitive decision-making, and when to use them. • Recognize the warning signs which could indicate breakdowns in safety-related decision-making processes and when/how to escalate a problem

Appendix B-3: Senior Management Workshop

(Two Day Session)

The Senior Management workshop training will expand on the topics introduced in the Senior Leadership Seminar.

The major focus of the workshop will consist of facilitated discussion of the CAIB report, focusing on the overall initiative to benchmark and improve the critical decision-making skills within NASA, including changing the decision-making culture agency-wide.

Topics will include: critical decision-making strategies, risk assessment, NASA safety culture (including socio/psychological group dynamics and influences), individual accountability within the system at NASA, dissenting/minority opinions, and leadership. The training will be highly interactive and participatory, enabling participants to immediately apply specific skills and techniques to their respective work environments.

Training methods used through the session will include: invited guest lecturers (i.e., Diane Vaughn, Gary Klein, etc.), case studies, dynamic group activity, group discussion, self-assessments, and problem solving.

Senior Management Workshop Outline

Day One Sessions	
8:30 a.m.	Introductions
9:00 a.m.	Knowledge Cafe *Break into teams, assigning topics to be discussed; rotate teams through topics for 6-8 minutes each Regroup and review results.*
10:00 a.m.	BREAK
10:15 a.m.	Columbia Lessons Learned Case Study
12:00 Noon	LUNCH
1:00 p.m.	Address by nationally-prominent expert
3:30 p.m.	BREAK
3:45 p.m.	Lessons from Tufte
4:45 p.m.	Review next day's plan and give homework assignment
5:00 p.m.	End of Day One
Day Two Sessions	
8:30 a.m.	Review of homework assignment
9:00 a.m.	Current NASA Culture - Reality Check *In small groups, answer the following question (30 minutes)*

	How would you describe the NASA decision-making culture? Consider the following: • *Are critical decisions made at the appropriate levels?* • *The overall communication environment, including flow of critical information to decision-makers.* • *How are minority/differing opinions handled?* • *How is risk assessed and/or managed?* • *The process for escalating safety concerns.* • *Relationship between NASA and contractor personnel.* *Reconvene as one group - identify patterns and discuss (30 minutes)*
10:00 a.m.	BREAK
10:15 a.m.	Decision-Making And Risk Assessment Models Present several decision-making techniques • *Analytic hierarchy process, etc.* • *Rational vs. intuitive processes* Discuss decision-making contexts • *Schedule: time critical vs. relaxed* • *Risk: high vs. low* • *Complexity: large amounts of information vs. small* • *Data: quantitative vs. qualitative, ambiguous vs. clear, incomplete vs. complete* • *Situation: dynamic vs. fixed* • *Affects of stress and conflict*
	Discuss Decision-Making Applications and Strategies • *Discussion – how/when to apply. Give examples. Concrete, practical strategies.* • *When should waivers be created? When should deviation from requirements be accepted?* • *Discuss how to recognize the warning signs which could indicate breakdowns in safety-related decision-making processes.* • *Identify paths of information flow to decision makers* • *When and how to escalate concerns or minority opinions?*
11:15 a.m.	**Group Activity** *Interactive group problem-solving activity that will surface leadership, group dynamics, teams, decision-making abilities, and individual conduct in small groups.* Discuss/Debrief: Each team describes what happened in their team *a. Who took on the role as leader? Other roles?* *b. What process did you use to come to a decision? Compare the process to the outcome.* *c. Would you do anything differently?* *d. Were there any minority factions?* *e. What made you successful/unsuccessful?* f. *What was your accountability in the outcome?*
12:00 Noon	LUNCH
1:00 p.m.	Dynamics of Groups Characteristics of group decision-making *Divergence/convergence, Collaboration*
1:20 p.m.	"Groupthink" Challenger Discussion View Challenger "Groupthink" Video Facilitated Discussion of Groups in NASA (One group) • *Where have you seen "groupthink" in action?* • *What groups/teams at NASA are working well/not working well?* • *Describe the role of individual accountability and leadership in group settings.*
2:00 p.m.	Take Leadership Style Assessment

	• *Interpret results.* • *Retrospective discussion of group activity – which styles did you spot?* • *Individual writing - define your organizational role.*
2:30 p.m.	BREAK
2:45 p.m.	Individual Accountability And Leadership A. Story of Monastery B. Role of individual in context of critical decision-making • *What's in it for you?* • *Discuss: Challenger video, Group activity.* • *Value of minority viewpoints.* • *Discuss Leadership and its contribution.* • *Apollo 13 clip – Ed Harris "Failure is not an option."*

Senior Management Workshop -- Focus Areas

Area	Action
Agency Culture	• Examine NASA, Enterprise, Center, and Program decision-making cultures. Identify recurring themes and patterns. • Review NASA's process for escalating safety concerns. • Identify techniques for developing, considering, and incorporating minority dissenting opinions. • Discuss relationships with contractors and how to evaluate accuracy of their decisions and program inputs • Analyze paths of information flow to decision-makers and define ways to improve accuracy and comprehensiveness.
Group Dynamics	• Examine models of group dynamics and collaborative decision-making, including socio/psychological components and "groupthink." • Participate in group-based learning scenarios, demonstrating collaborative decision-making techniques.
Decision-making Techniques and Strategies	• Understand and apply simple decision-making techniques. • Discuss the differences between analytical and intuitive decision-making, and when to use them. • Recognize the warning signs which could indicate breakdowns in safety-related decision-making processes and when/how to escalate a problem.
Individual Roles & Accountability	• Spotlight individual roles and accountability in decision-making processes. Gain awareness of one's own behavior and how it is influenced by – and influences – groups. • Discuss current issues facing participants; identify what is working and not working, both in culture and in process. • Identify changes to one's own behavior that could improve decision-making effectiveness and have a positive impact on Agency culture.

This page intentionally blank.

Appendix B-4: Program/Project Team Workshop

(Three Day Session)

The Program/Project Team Workshop training will expand on the topics introduced in the Senior Management Workshop.

The major focus of the workshop is to benchmark and improve the critical decision-making skills within NASA, with a long-term goal of changing the decision-making culture Agency-wide.

Topics will include: critical decision-making strategies, risk assessment, NASA safety culture (including socio/psychological group dynamics and influences), individual accountability within the system at NASA, dissenting/minority opinions, and leadership. The training will be highly interactive and participatory, enabling participants to immediately apply specific skills and techniques to their respective work environments.

Training methods used through the session will include: lecturer facilitated group discussions, case studies, self-assessments, and problem solving.

Program/Project Team Workshop Outline

Time	Day One
8:30 a.m.	Welcome and Introductions
9:00 a.m.	Current NASA Culture - Reality Check *Knowledge Café: answer the following questions (60 minutes)* • *How are critical decisions made in your organization?* • *Describe the overall communication environment, including flow of critical information to decision-makers.* • *What is your organization's attitude towards voicing minority opinions or concerns?* • *How is risk assessed and/or managed?* *Reconvene as one group - identify patterns and discuss*
10:30 a.m.	BREAK
10:15 a.m.	Decision-Making Strategies *Discuss decision-making in the context of the NASA culture(s)* • *Schedule: time critical vs. relaxed* • *Risk: high vs. low* • *Complexity: large amounts of information vs. small* • *Data: quantitative vs. qualitative, ambiguous vs. clear, incomplete vs. complete* • *Situation: dynamic vs. fixed* • *Affects of stress and conflict*
	Discuss Decision-Making Applications and Strategies • *Discussion – how/when to apply. Give examples. Concrete, practical strategies.* • *When should waivers be created? When should deviation from requirements be*

	accepted? • *Discuss how to recognize the warning signs which could indicate breakdowns in safety-related decision-making processes.* • *Identify paths of information flow to decision makers.* • *When and how to escalate concerns or minority opinions?*
Noon	LUNCH
1:00 p.m.	**Group Activity** *Interactive group problem-solving activity that will surface leadership, group dynamics, teams, decision-making abilities, and individual conduct in small groups.* *Discuss/Debrief: Each team describes what happened in their team* • *Who took on the role as leader? Other roles?* • *What process did you use to come to a decision? Compare the process to the outcome.* • *Would you do anything differently?* • *Were there any minority factions?* • *What made you successful/unsuccessful?*
2:00 p.m.	**"Challenger" Video and Discussion** *View Challenger Video* *Facilitated Discussion of the decision process illustrated in the video* • *What group decision-making characteristics do you recognize from the video?* • *What groups/teams at NASA are working well/not working well?* • *Describe the role of individual accountability and leadership in group settings.*
3:30 p.m.	**Take Leadership Style Assessment** • *Interpret results.* • *Retrospective discussion of group activity – which styles did you spot?* • *Individual writing - define your organizational role.*
4:30 p.m.	**ADJOURN**

8:30 a.m.	**Day Two**
8:45 a.m.	Individual Accountability and Leadership *Role of individual in context of critical decision-making* • *Discuss: Value of minority viewpoints* • *Discuss: Leadership, and its contribution*
9:15 a.m.	Dynamics of Groups in Collaborative Decision-Making *Characteristics of group decision-making* • *Divergence/convergence, Collaboration*
10: 15 a.m.	BREAK
10:30 a.m.	Introduce Case Study Complex high-risk NASA case study that addresses all prior-covered information. Contains: Schedule pressure, budgetary pressure, data ambiguity, and stakeholder disagreement. Participants will have to come to a consensus and decision. Discuss.
11:15 a.m.	Groups Considerations *Conflict* *Case Study and Discussion*
Noon	LUNCH
1:00 p.m.	Introduce the 3-Step Decision Engineering Model

	Applicability • *What's in it for you?*
1:15 p.m.	Step One: Decision Framing *Context* *Applicability* *Examples* • *Case Study* • *Case Study Discussion*
2: 30 p.m.	BREAK
2:45 p.m.	Perceptions of Opportunity and Risk in Decision-Making *Context* *Theory* *Practical Applications* • *Group Activities* • *Case Study*
4:30 p.m.	ADJOURN

8:30 a.m.	**Day Three**
8:45 a.m.	Step Two: Generating Alternatives *Role of alternatives in context of critical decision-making* *Alternative Generation Techniques* • *Case Study and Group Discussion* • *Apollo 13 clip*
10: 30 a.m.	BREAK
10:30 a.m.	Step Three: Decide the Course of Action *Rational versus Intuitive decision processes* • *Applicability* *Rational Techniques* • *Analytical Hierarchy Process (AHP)* • *Multi Attribute Utility Theory (MAUT)* • *Decision Trees and Bayesian Analysis*
Noon	**LUNCH**
1:00 p.m.	Intuitive Techniques *Simulations* *Pre-Mortem/Scenario Planning* • *Case Study and Discussion*
2:00 p.m.	**Decision Traps and Cognitive Biases** *"Group Think"* *Anchoring* *Confirming Evidence* *Status Quo* *Other common biases* • *Class Activity* • *Case Study and Discussion*
2: 45 p.m.	BREAK
3:00 p.m.	Generate Individual Action Plans *Each participant identifies, in writing, where, in their job performance, they would apply the*

	concepts from this workshop. These will then be used in follow-on activities at a later date.
3:30 p.m.	Course Summary and Wrap Up *Review of Learning Objectives* *Course evaluation* *Discuss next steps in overall initiative*
4:30 p.m.	ADJOURN

Project Team Workshop – Focus Areas

Area	**Action**
Agency Culture	• Examine NASA, Enterprise, Center, and Program decision-making cultures. Identify recurring themes and patterns. • Review NASA's process for escalating safety concerns. • Identify techniques for developing, considering, and incorporating minority dissenting opinions. • Discuss relationships with contractors and how to evaluate accuracy of their decisions and program inputs • Analyze paths of information flow to decision-makers and define ways to improve accuracy and comprehensiveness.
Group Dynamics	• Examine models of group dynamics and collaborative decision-making, including socio/psychological components and "groupthink." • Participate in group-based learning scenarios, demonstrating collaborative decision-making techniques.
Decision-making Techniques and Strategies	• Understand and apply simple decision-making techniques. • Discuss the differences between analytical and intuitive decision-making, and when to use them. • Recognize the warning signs which could indicate breakdowns in safety-related decision-making processes, and when/how to escalate a problem
Individual Roles & Accountability	• Spotlight individual roles and accountability in decision-making processes. Gain awareness of one's own behavior and how it is influenced by – and influences – groups. • Discuss current issues facing participants; identify what is working and not working, both in culture and in process. • Identify changes to one's own behavior that could improve decision-making effectiveness and have a positive impact on Agency culture.

APPENDIX C: NNBE Memoranda of Agreement (MOA)

Appendix C-1: Quality Assurance Agreement

MEMORANDUM OF AGREEMENT
BETWEEN THE
UNITED STATES NAVY
NAVAL SEA LOGISTICS CENTER DETACHMENT PORTSMOUTH, NH
AND
OFFICE OF SAFETY AND MISSION ASSURANCE
HEADQUARTERS
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
WASHINGTON, DC

1. PURPOSE. This Memorandum of Agreement (MOA) is between the Naval Sea Logistics Center Detachment, Portsmouth, NH (herein referred to as NAVSEALOGCENDET Portsmouth) and the Office of Safety and Mission Assurance, Headquarters, National Aeronautics and Space Administration, Washington, DC, (herein referred to as NASA). This agreement provides for NASA, including its field activities, the use of the Navy's web-accessible, Product Data. Reporting and Evaluation Program (PDREP), and the web-accessible Red/Yellow/Green (RYG) Program. NAVSEALOGCENDET Portsmouth will provide NASA with web-access to the PDREP Automated Information System (AIS) to store NASA product quality information, and the RYG program to store delivery data. NASA will have use of both programs per the terms of this agreement.

2. AUTHORITY. The authority for NASA entering into this MOA is section 203(c) of the National Aeronautics and Space Act of 1958, as amended [42 U.S.C. § 2473(c)] and the Economy Act [31 U.S.C. § 1535].

3. RESPONSIBILITIES.

a. NAVSEALOGCENDET Portsmouth will use reasonable efforts to:

(1) Make changes to the PDREP database, as required to support NASA use (e.g., addition of NASA quality information codes, inclusion of delivery data, change to RYG and User Profile to display NASA Reporting Activities for NASA records).

(2) Based on NASA input, store closed, contractor-liable, defect-verified quality data and delivery information for NASA to be used for program management reports.

(3) Conduct test sweeps to validate NASA data prior to utilizing in program management tools.

(4) Provide technical support to NASA users on PDREP on an as-needed basis.

(5) Provide web access to PDREP and RYG (user name/password) to identified NASA users.

(6) Ensure C2 level of security in accordance with DoD 5200.28, Security Requirements for Automated Information Systems.

(7) Provide NASA user training on a fee for service basis.

(8) Provide identified NASA users access to the PDREP database in order to run query reports.

b. The Office of Safety and Mission Assurance at NASA Headquarters will use reasonable efforts to:

(1) Reimburse NAVSEALOGCENDET Portsmouth for the costs incurred to fulfill unique NASA requirements/PDREP/RYG program changes, maintenance, training, travel, and support of NASA data in the PDREP/RYG database (see Appendix A). Unique requirements that require reimbursement by NASA will be agreed to by both NASA and the NAVSEALOGCENDET Portsmouth in writing prior to fulfillment of each such requirement.

(2) Arrange for the sending of quality data and delivery data (in the NAVSEALOGCENDET Portsmouth requested format) to a NAVSEALOGCENDET Portsmouth FTP Server between the 20th and 25th of each month, for use in the leading indicator process.

(3) Provide NAVSEALOGCENDET Portsmouth with a Point of Contact at each NASA Center for quality information and delivery concerns.

(4) Promote the use of PDREP/RYG throughout NASA.

(5) Identify NASA users authorized to access PDREP/RYG.

(6) Serve as the interface between NASA and the Navy for oversight of the activities covered by this agreement.

4. LEVEL OF SUPPORT. The level of NAVSEALOGCCENDET Portsmouth support and services will be commensurate with the NASA funding provided. NASA will reimburse for actual support services rendered. All activities under or pursuant to this MOA are subject to the availability of appropriated funds and no provision shall be interpreted to require obligation or provision of funding in violation of the Anti-Deficiency Act [31 U.S.C. § 1341]. Funding will be accomplished via a

mutually agreeable separate funding instrument under the Economy Act. Support services and their associated cost estimates are shown in Appendix A. NASA will provide advance funding in quarterly increments, prior to the accomplishment of requested support services. NASA funding documents shall be forwarded to the following address with an advanced (fax) copy provided to Ms. Joanne Rollins, NAVSEALOGCENDET Portsmouth, tel. 603.431.9460, x452, Fax 603.431.9464.

UIC 65538
John Betts, N01F 717.605.3132, Fax: 717.605.1780
Naval Sea Logistics Center
PO Box 2060, 5450 Carlisle Pike
Mechanicsburg, PA 17055-0795

5. ALLOCATION OF RISK. Each party agrees to assume liability for its own risks associated with activities under or pursuant to this MOA.

6. ANNUAL REVIEW. Each year a review of this MOA will be conducted between the parties. The parties intend these reviews to take place one quarter prior to the beginning of the new fiscal year. The first review will be in the first full year fiscal year of activity. The purposes of the review will be to:

a. Reaffirm organizational commitment to the project and review agreement.

b. Review previous year's actual project/task costs versus estimates.

c. Discuss changes, including adjustments in prices/labor rates.

d. Balance planned levels of support for the upcoming fiscal year with available funding levels.

7. POINTS OF CONTACT. The individuals named below shall serve as the respective points of contact for all correspondence pertaining to this MOA:

NASA:

Name:	Tom Whitmeyer
Title:	Manager, Agency Quality Assurance Program
Address:	NASA Headquarters, Washington DC 20024
Tel:	202.358.2228
Fax:	202.358.3104
E-mail:	tom.whitmeyer@hq.nasa.gov

NAVSEALOGCENDET Portsmouth:

Name:	Duncan MacDonald
Title:	PDREP Project Manager
Address:	Naval Sea Logistics Center Detachment Portsmouth

80 Daniel Street, Suite 400
Portsmouth, NH 03801-3884
Tel: (603).431.9460, x462 or DSN 684.1371, x462
Fax: (603).431.9464
E-mail: macdonalddl@navsea.navy.mil

NAVSEALOGCENDET Portsmouth:
Name: Wendell T. Smith III
Title: Acquisition Support Programs Product Manager
Address: Naval Sea Logistics Center Detachment Portsmouth
80 Daniel Street, Suite 400
Portsmouth, NH 03801-3884
Tel: 603.431.9460, x451 or DSN 684.1371, x451
Fax: 603.431.9464
E-mail: smithwt1@navsea.navy.mil

8. EFFECTIVE DATE OF AGREEMENT. This MOA shall be effective upon signature of all parties and will remain in force for 5 years unless terminated by either party with 3 months written notice. The terms of this agreement may be extended after 5 years, if mutually agreed to by all parties though an amendment to this agreement. Any party may request the initiation of a review and/or an amendment at any time should changing conditions warrant. Any amendment to this agreement shall be in writing and approved by the signatories. Written modifications to Appendix A may be made at the Program Manager level provided that there are no significant budget impacts and the modifications are approved by both parties.

Bryan D O'Connor
Bryan D. O'Connor Date 11 JUN 03
Associate Administrator,
Office of Safety and Mission Assurance
NASA Headquarters

Wendell T. Smith III 25 June '03
Wendell T. Smith III Date
Acquisition Support Product Manager
Naval Sea Logistics Center Detachment,
Portsmouth

Stephen M Bonwich 26 JUNE 03
Stephen M. Bonwich Date
Executive Director
Logistics, Maintenance and Industrial Operations
Naval Sea Systems Command

Attachment to Appendix C-1 (referred to as “Appendix A” in Memo Text)

For Combined Navy/NASA PDREP/RYG*

FY03 One Time Costs for single source data is estimated to be approx. $35K and includes:

Programming/Analysis for Test File
Includes programming table mods, data load/transfer, profile changes, and generation of test file for review of Navy and Navy/NASA ratings.

QA Vendor Test and Validation
Audit monthly sweep, notify NASA contractors, go through rebuttal process, verify accuracy and validity of data.

On-Site Customer Training: Fee-for-service based on location, number of sites, duration and personnel.
Conduct on-site training sessions.

FY03 Recurring Costs for single source data is estimated to be approx. $100K/FY* and includes:

Run data sweeps monthly and make reports available to designated NASA program representatives.

Program Management/Oversight

PDREP Database/Sys Ops
Includes database storage, license fees, system maintenance, facility/communication links, help desk support, data transfer validations, sweep administration, user-ids/passwords, travel and supplies.

* FY03 cost will be prorated and dependent upon implementation date.

NOTE: For planning purposes, FY04 and out year costs can be estimated by applying a 5 % inflation factor and will be further adjusted to reflect NASA-requested unique requirements; e.g., programming over and above normal enhancements and any additional requested fee-for-service training.

This page intentionally blank.

Appendix C-2: Engineering Investigations and Analyses Agreement

MEMORANDUM OF AGREEMENT
BETWEEN THE
UNITED STATES NAVY
NAVAL SEA SYSTEMS COMMAND
AND THE
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
FOR PARTICIPATION IN ENGINEERING INVESTIGATIONS & ANALYSES

1. PURPOSE. This Memorandum of Agreement (MOA) is between the Naval Sea Systems Command, Washington, DC (herein referred to as NAVSEA) and the National Aeronautics and Space Administration, Washington, DC, Office of Safety and Mission Assurance (herein referred to as NASA). Hereinafter, NASA and NAVSEA will also be referred to individually as Party or collectively as Parties.

This agreement provides NASA and its field activities, and NAVSEA and its field activities reciprocal rights to participate in the conduct of mutually agreed, on-going or newly created engineering investigations and analyses of programs and projects. The participation by one Party in the other Party's programs/projects will be governed by the mission, sensitivity, security, safety, and national security considerations associated with that program/project and will be conducted solely at the invitation of the Party whose program/project is undergoing the engineering investigation analysis. The intent of this MOA is to allow each Party to participate in (contribute) and learn from the other Party's processes.

2. AUTHORITY. The authority for NASA entering into this MOA is section 203(c) of the National Aeronautics and Space Act of 1958, as amended [42 U.S.C. § 2473(c)].

3. RESPONSIBILITIES.

a. NAVSEA shall:

(1) Identify opportunities for NASA participation in NAVSEA engineering investigations and analyses of submarine programs/projects.

(2) For those programs/projects identified, provide points of contact to assist in the processing, coordination, and conduct of NASA participation.

(3) Establish the number of NASA participants desired for each program/project analysis/investigation by experience level and expertise and identify access/security clearance requirements.

(4) Make available to NASA, on-site and read-ahead information to enhance the NASA participant's understanding of Navy terminology, policy, procedures and practices in advance of the actual participation.

(5) For any Investigations/Analyses identified that relate to Reactor Safety, coordinate the program/project with NAVSEA 08 Naval Reactors.

b. NASA shall:

(1) Identify opportunities for NAVSEA participation in NASA engineering investigations and analyses of NASA aerospace programs/projects.

(2) For those programs/projects identified, provide points of contact to assist in the processing, coordination, and conduct of NAVSEA participation.

(3) Establish the number of NAVSEA participants desired for each program/project analysis/investigation by experience level and expertise and identify access/security clearance requirements.

(4) Make available to NAVSEA on-site and read-ahead information to enhance NAVSEA understanding of NASA terminology, policy, procedures and practices in advance of the actual participation.

4. LEVEL OF PARTICIPATION. The level of participation in each Party's program/project (number of participants, experience, expertise and length of time) will be mutually agreed in writing by both NAVSEA and NASA in advance of the investigation/analysis initiation date. Each Party will provide its own support and funding and will share the knowledge gained from such participation with the interfacing organization. All activities under or pursuant to this MOA are subject to the availability of personnel and resources to support their respective participation and to limitations on participation by the hosting activity.

5. FINANCIAL OBLIGATIONS. Each party will fund its own participation under this MOA. subject to the availability of funds. No provision shall be interpreted to require obligation or provision of funding in violation of the Anti-Deficiency Act [31 U.S.C. § 1341].

6. COMPLIANCE WITH LAWS. Each Party recognizes its responsibility to comply with all Federal laws and regulations applicable to each Party's performance of the activities under this MOA. In the event that this Agreement conflicts or is inconsistent with any Federal law or regulation, such Federal laws and regulations shall govern.

7. ALLOCATION OF RISK. Each Party agrees to assume liability and hold the other party harmless against any and all liability for its own risks associated with activities performed under or pursuant to this MOA. All costs, expenses, or liabilities of a Party caused by or arising out of activities performed under this MOA shall be borne solely by that Party. Neither Party to this MOA shall be liable to the other Party for any costs, expenses, or liabilities for which the other Party is solely responsible.

8. ANNUAL REVIEW. This MOA will be reviewed yearly, with the reviews taking place one calendar quarter prior to the beginning of the new fiscal year. The purposes of the review will be to:

a. Reaffirm organizational commitment to the agreement.

b. Review previous year's actual participation and share lessons learned to strengthen each other's engineering investigation and analysis processes.

9. POINTS OF CONTACT. The individuals named below shall serve as the respective points of contact for all correspondence pertaining to this MOA:

NASA:

Name: J. Steven Newman
Title: Senior Technical Advisor
Address: NASA Headquarters,
Washington DC 20024
Tel: 202.358.1408
Fax: 202.358.2778
E-mail: snewman@hq.nasa.gov

NAVSEA HQ Washington:

Name: James M. Lawrence
Title: Ship Design Manager for In-service Submarines
Address: Naval Sea Systems Command
ATTN: 05U3
614 Sicard Street SE, Stop 7002
Washington Navy Yard
Washington, DC 20376-7002
Tel: 202.781.3409
Fax: 202.781.4669
E-mail: lawrencejm@navsea.navy.mil

10. RELEASE OF INFORMATION. Information furnished between the Parties (whether documentary, oral, visual or otherwise) shall be considered business sensitive and/or business confidential and used only for the purposes of performing the projects/programs that are the subject of this MOA. Neither Party to this MOA shall modify, reproduce, display, disclose or release information derived from the other Party to a non-participating third party without the prior written approval of the contributing MOA Party. Furthermore, each Party agrees not to use any information obtained as a result of the activities performed under this MOA in any manner that is inconsistent with the purposes specified herein. Each Party agrees to establish or use existing operating procedures and physical security measures designed to protect information derived or obtained from

the other Party from inadvertent release or disclosure to unauthorized third parties. This provision shall survive the termination or expiration of this agreement.

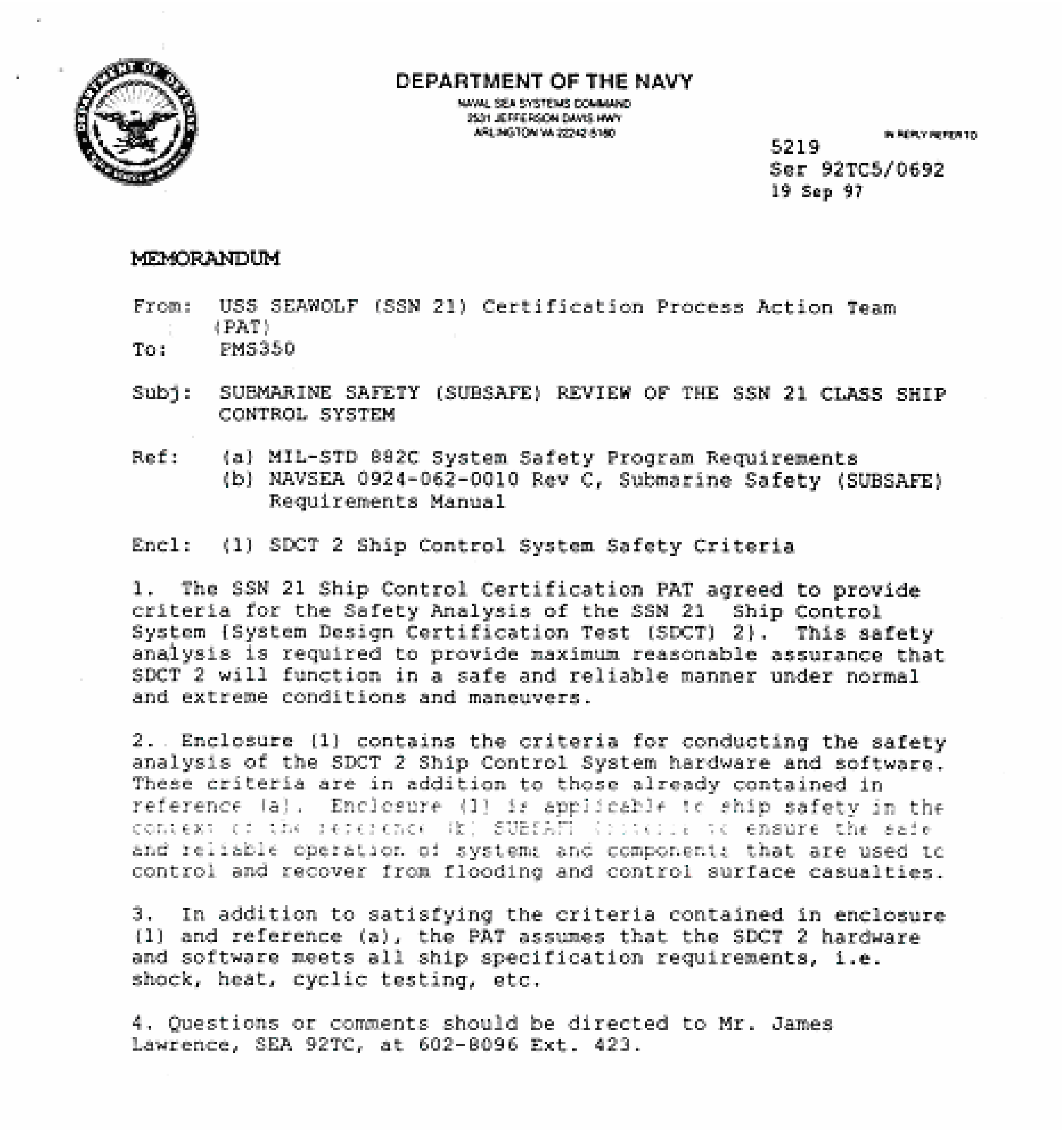
11. EFFECTIVE DATE OF AGREEMENT. This MOA shall be effective upon signature of both Parties and will remain in force for 5 years from the execution date of the last signatory unless terminated by either Party with 3 months written notice. The terms of this agreement may be extended after 5 years if mutually agreed to in writing by both Parties. Either Party may initiate review and/or a modification at any time should changing conditions warrant. Any modification or amendment to this agreement shall be in writing and approved by the signatories.

Bryan O'Connor 2DEC03
Bryan D. O'Connor Date
Associate Administrator
NASA Office of Safety and Mission Assurance
NASA Headquarters, Washington, DC

12/2/03
Gregg Hagedorn Date
Executive Director Ship Design,
Integration and Engineering
NAVSEA Headquarters , Washington, DC

APPENDIX D: Navy Memos outlining Software Safety Criteria

Appendix D-1: Seawolf Class Software Safety Criteria



DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
2531 JEFFERSON DAVIS HWY
ARLINGTON VA 22242-5160

IN REPLY REFER TO
5219
Ser 92TC5/0692
19 Sep 97

MEMORANDUM

From: USS SEAWOLF (SSN 21) Certification Process Action Team (PAT)
To: PMS350

Subj: SUBMARINE SAFETY (SUBSAFE) REVIEW OF THE SSN 21 CLASS SHIP CONTROL SYSTEM

Ref: (a) MIL-STD 882C System Safety Program Requirements
(b) NAVSEA 0924-062-0010 Rev C, Submarine Safety (SUBSAFE) Requirements Manual

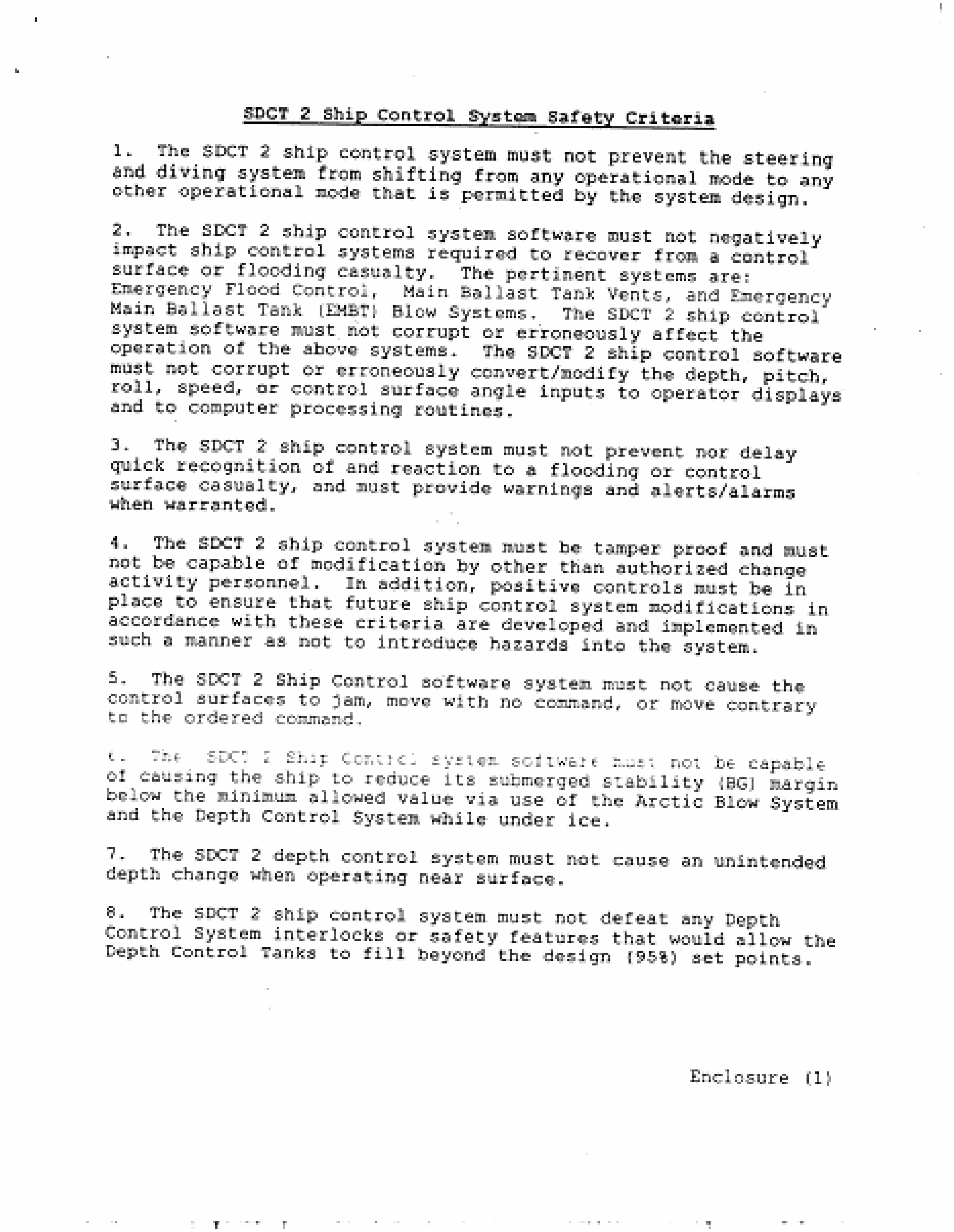
Encl: (1) SDCT 2 Ship Control System Safety Criteria

1. The SSN 21 Ship Control Certification PAT agreed to provide criteria for the Safety Analysis of the SSN 21 Ship Control System (System Design Certification Test (SDCT) 2). This safety analysis is required to provide maximum reasonable assurance that SDCT 2 will function in a safe and reliable manner under normal and extreme conditions and maneuvers.

2. Enclosure (1) contains the criteria for conducting the safety analysis of the SDCT 2 Ship Control System hardware and software. These criteria are in addition to those already contained in reference (a). Enclosure (1) is applicable to ship safety in the context of the reference (b) SUBSAFE criteria to ensure the safe and reliable operation of systems and components that are used to control and recover from flooding and control surface casualties.

3. In addition to satisfying the criteria contained in enclosure (1) and reference (a), the PAT assumes that the SDCT 2 hardware and software meets all ship specification requirements, i.e. shock, heat, cyclic testing, etc.

4. Questions or comments should be directed to Mr. James Lawrence, SEA 92TC, at 602-8096 Ext. 423.



SDCT 2 Ship Control System Safety Criteria

1. The SDCT 2 ship control system must not prevent the steering and diving system from shifting from any operational mode to any other operational mode that is permitted by the system design.

2. The SDCT 2 ship control system software must not negatively impact ship control systems required to recover from a control surface or flooding casualty. The pertinent systems are: Emergency Flood Control, Main Ballast Tank Vents, and Emergency Main Ballast Tank (EMBT) Blow Systems. The SDCT 2 ship control system software must not corrupt or erroneously affect the operation of the above systems. The SDCT 2 ship control software must not corrupt or erroneously convert/modify the depth, pitch, roll, speed, or control surface angle inputs to operator displays and to computer processing routines.

3. The SDCT 2 ship control system must not prevent nor delay quick recognition of and reaction to a flooding or control surface casualty, and must provide warnings and alerts/alarms when warranted.

4. The SDCT 2 ship control system must be tamper proof and must not be capable of modification by other than authorized change activity personnel. In addition, positive controls must be in place to ensure that future ship control system modifications in accordance with these criteria are developed and implemented in such a manner as not to introduce hazards into the system.

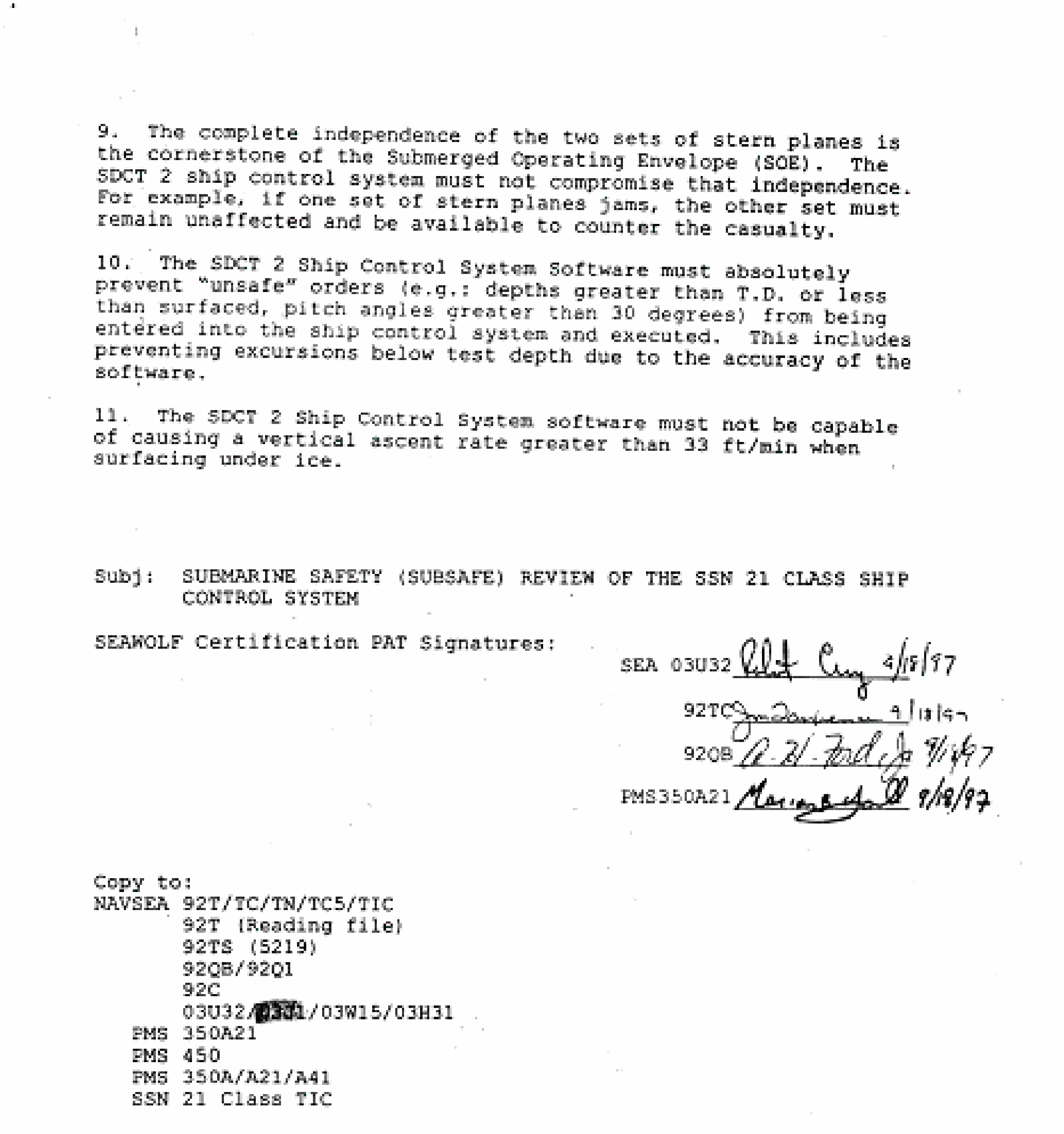
5. The SDCT 2 Ship Control software system must not cause the control surfaces to jam, move with no command, or move contrary to the ordered command.

6. The SDCT 2 Ship Control system software must not be capable of causing the ship to reduce its submerged stability (BG) margin below the minimum allowed value via use of the Arctic Blow System and the Depth Control System while under ice.

7. The SDCT 2 depth control system must not cause an unintended depth change when operating near surface.

8. The SDCT 2 ship control system must not defeat any Depth Control System interlocks or safety features that would allow the Depth Control Tanks to fill beyond the design (95%) set points.

Enclosure (1)



9. The complete independence of the two sets of stern planes is the cornerstone of the Submerged Operating Envelope (SOE). The SDCT 2 ship control system must not compromise that independence. For example, if one set of stern planes jams, the other set must remain unaffected and be available to counter the casualty.

10. The SDCT 2 Ship Control System Software must absolutely prevent "unsafe" orders (e.g.: depths greater than T.D. or less than surfaced, pitch angles greater than 30 degrees) from being entered into the ship control system and executed. This includes preventing excursions below test depth due to the accuracy of the software.

11. The SDCT 2 Ship Control System software must not be capable of causing a vertical ascent rate greater than 33 ft/min when surfacing under ice.

Subj: SUBMARINE SAFETY (SUBSAFE) REVIEW OF THE SSN 21 CLASS SHIP CONTROL SYSTEM

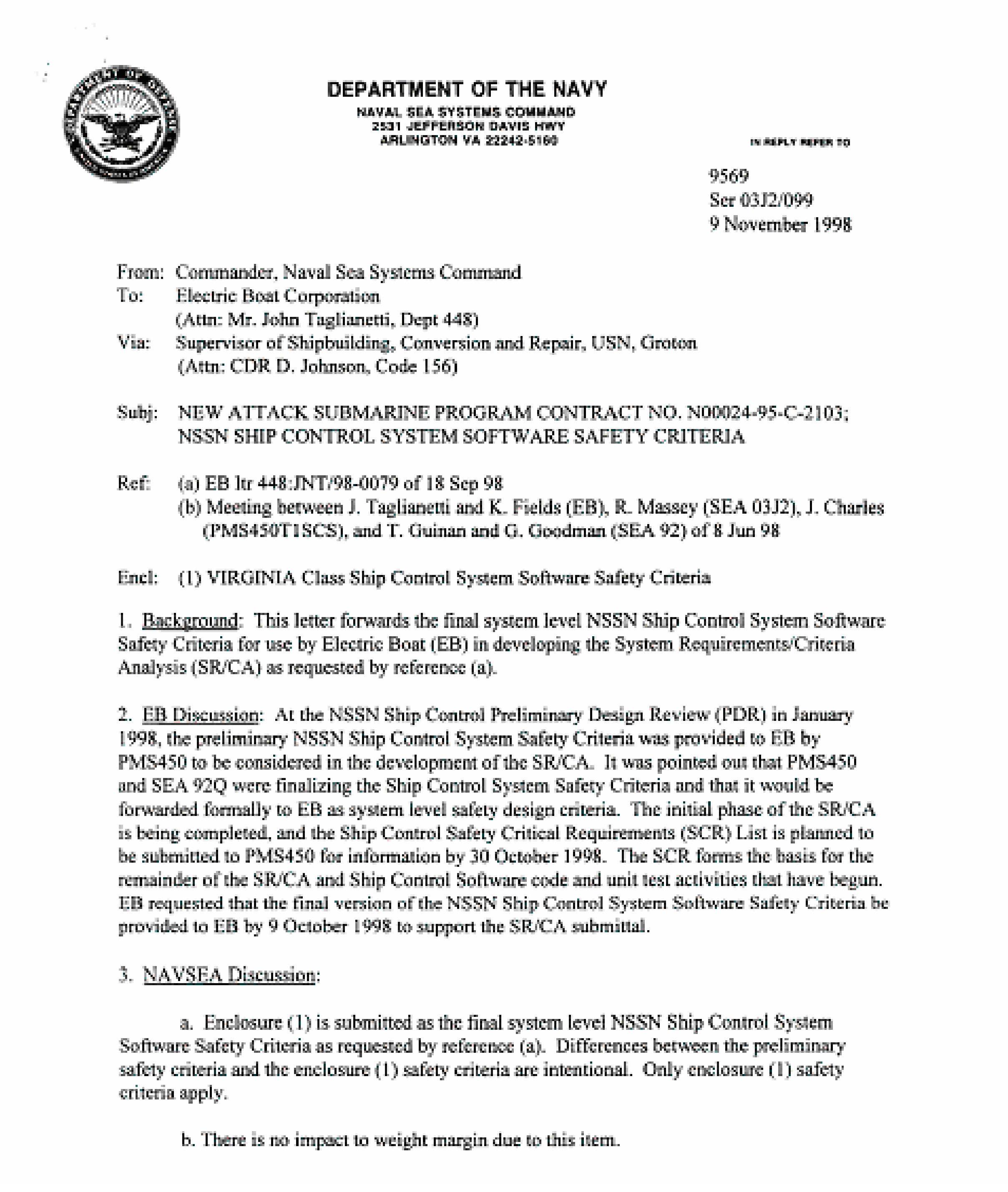
SEAWOLF Certification PAT Signatures:

SEA 03U32 4/15/97
92TC 9/18/97
92QB 9/18/97
PMS350A21 9/18/97

Copy to:
NAVSEA 92T/TC/TN/TC5/TIC
92T (Reading file)
92TS (5219)
92QB/92Q1
92C
03U32/[redacted]/03W15/03H31
PMS 350A21
PMS 450
PMS 350A/A21/A41
SSN 21 Class TIC

This page intentionally blank.

Appendix D-2: Virginia Class Software Safety Criteria



DEPARTMENT OF THE NAVY
NAVAL SEA SYSTEMS COMMAND
2531 JEFFERSON DAVIS HWY
ARLINGTON VA 22242-5160

IN REPLY REFER TO

9569
Ser 03J2/099
9 November 1998

From: Commander, Naval Sea Systems Command
To: Electric Boat Corporation
(Attn: Mr. John Taglianetti, Dept 448)
Via: Supervisor of Shipbuilding, Conversion and Repair, USN, Groton
(Attn: CDR D. Johnson, Code 156)

Subj: NEW ATTACK SUBMARINE PROGRAM CONTRACT NO. N00024-95-C-2103;
NSSN SHIP CONTROL SYSTEM SOFTWARE SAFETY CRITERIA

Ref: (a) EB ltr 448:JNT/98-0079 of 18 Sep 98
(b) Meeting between J. Taglianetti and K. Fields (EB), R. Massey (SEA 03J2), J. Charles (PMS450T1SCS), and T. Guinan and G. Goodman (SEA 92) of 8 Jun 98

Encl: (1) VIRGINIA Class Ship Control System Software Safety Criteria

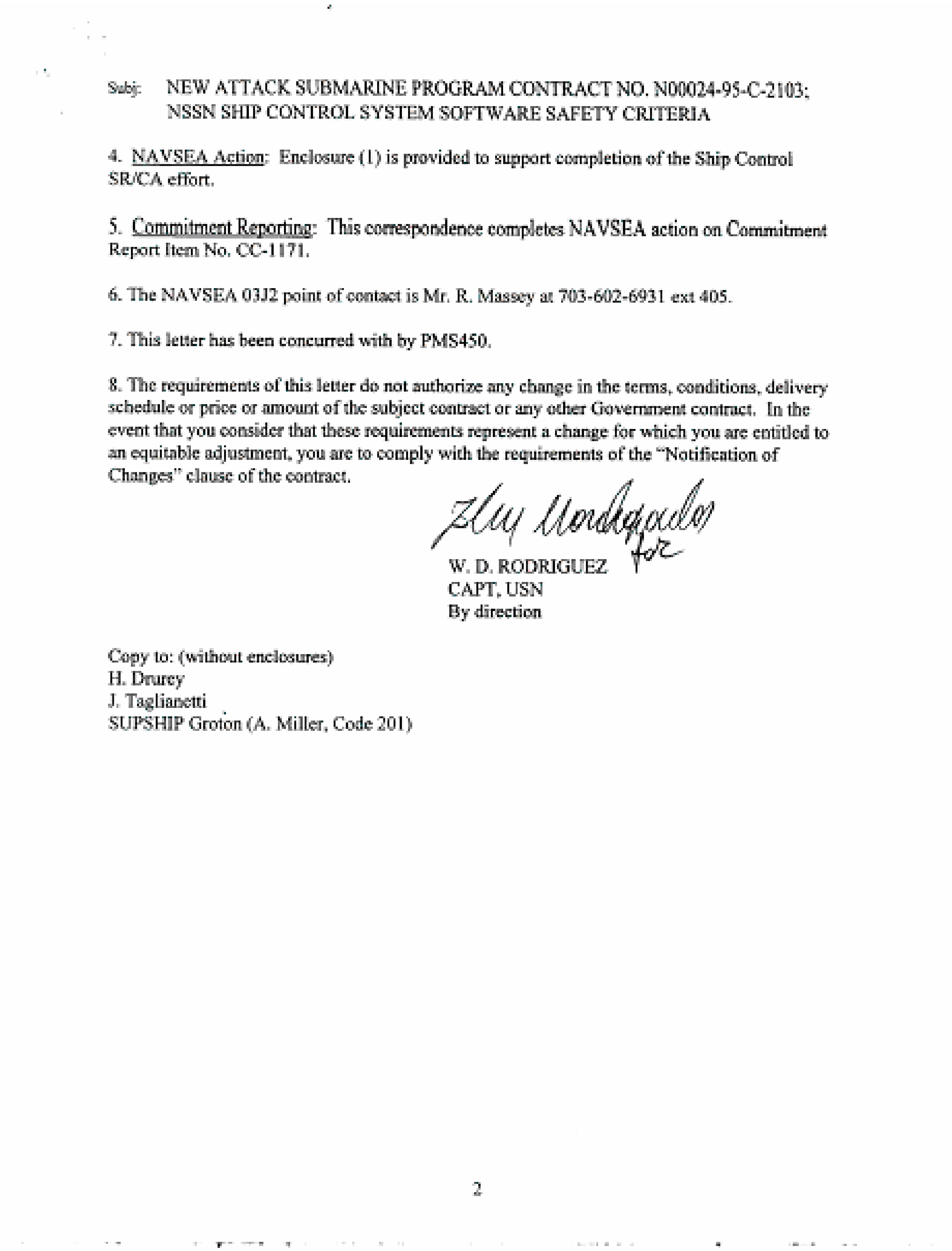
1. Background: This letter forwards the final system level NSSN Ship Control System Software Safety Criteria for use by Electric Boat (EB) in developing the System Requirements/Criteria Analysis (SR/CA) as requested by reference (a).

2. EB Discussion: At the NSSN Ship Control Preliminary Design Review (PDR) in January 1998, the preliminary NSSN Ship Control System Safety Criteria was provided to EB by PMS450 to be considered in the development of the SR/CA. It was pointed out that PMS450 and SEA 92Q were finalizing the Ship Control System Safety Criteria and that it would be forwarded formally to EB as system level safety design criteria. The initial phase of the SR/CA is being completed, and the Ship Control Safety Critical Requirements (SCR) List is planned to be submitted to PMS450 for information by 30 October 1998. The SCR forms the basis for the remainder of the SR/CA and Ship Control Software code and unit test activities that have begun. EB requested that the final version of the NSSN Ship Control System Software Safety Criteria be provided to EB by 9 October 1998 to support the SR/CA submittal.

3. NAVSEA Discussion:

a. Enclosure (1) is submitted as the final system level NSSN Ship Control System Software Safety Criteria as requested by reference (a). Differences between the preliminary safety criteria and the enclosure (1) safety criteria are intentional. Only enclosure (1) safety criteria apply.

b. There is no impact to weight margin due to this item.



Subj: NEW ATTACK SUBMARINE PROGRAM CONTRACT NO. N00024-95-C-2103;
NSSN SHIP CONTROL SYSTEM SOFTWARE SAFETY CRITERIA

4. NAVSEA Action: Enclosure (1) is provided to support completion of the Ship Control SR/CA effort.

5. Commitment Reporting: This correspondence completes NAVSEA action on Commitment Report Item No. CC-1171.

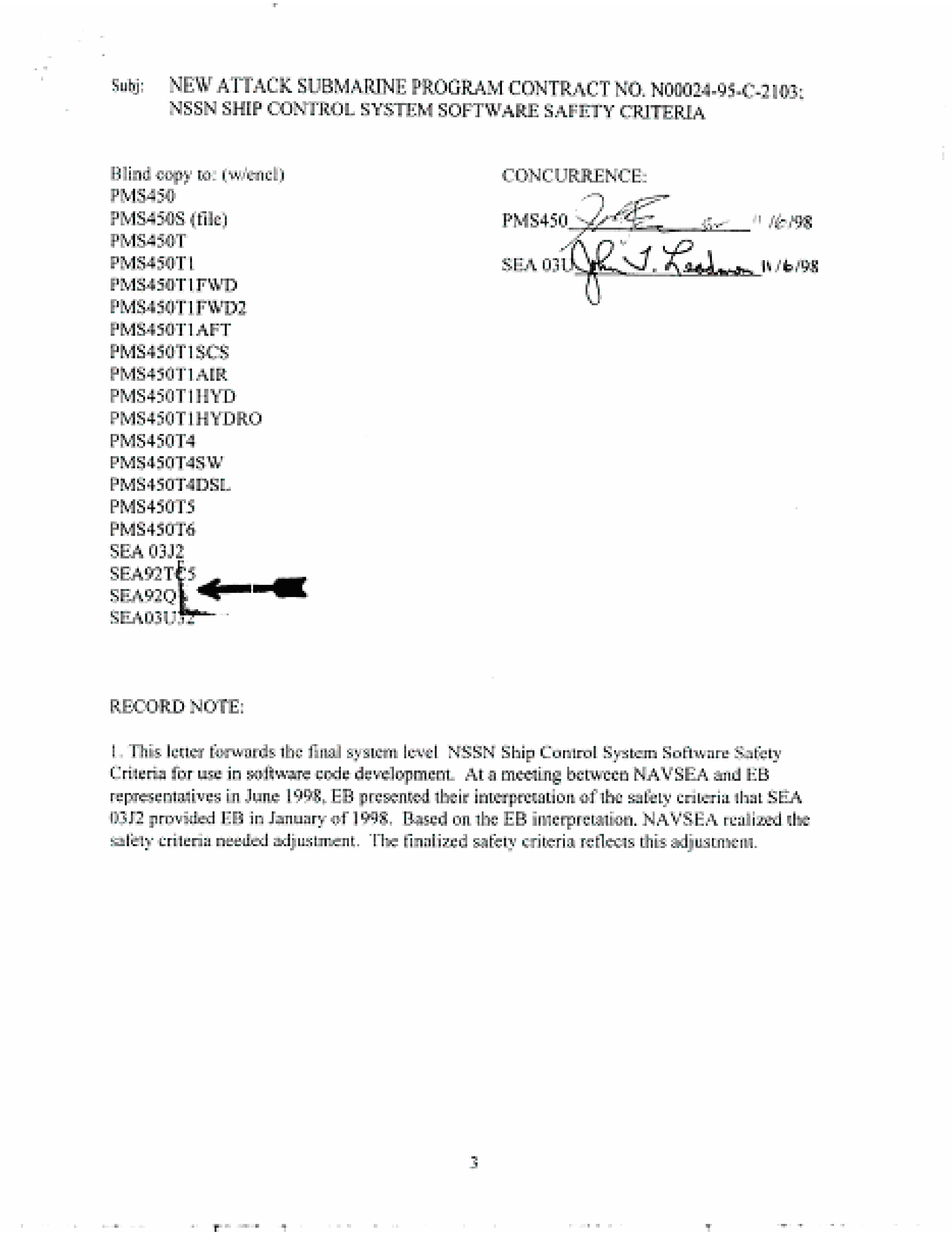
6. The NAVSEA 03J2 point of contact is Mr. R. Massey at 703-602-6931 ext 405.

7. This letter has been concurred with by PMS450.

8. The requirements of this letter do not authorize any change in the terms, conditions, delivery schedule or price or amount of the subject contract or any other Government contract. In the event that you consider that these requirements represent a change for which you are entitled to an equitable adjustment, you are to comply with the requirements of the "Notification of Changes" clause of the contract.

W. D. RODRIGUEZ
CAPT, USN
By direction

Copy to: (without enclosures)
H. Drurey
J. Taglianetti
SUPSHIP Groton (A. Miller, Code 201)



Subj: NEW ATTACK SUBMARINE PROGRAM CONTRACT NO. N00024-95-C-2103:
NSSN SHIP CONTROL SYSTEM SOFTWARE SAFETY CRITERIA

Blind copy to: (w/encl)
PMS450
PMS450S (file)
PMS450T
PMS450T1
PMS450T1FWD
PMS450T1FWD2
PMS450T1AFT
PMS450T1SCS
PMS450T1AIR
PMS450T1HYD
PMS450T1HYDRO
PMS450T4
PMS450T4SW
PMS450T4DSL
PMS450T5
PMS450T6
SEA 03J2
SEA92TC5
SEA92Q
SEA03UJ2

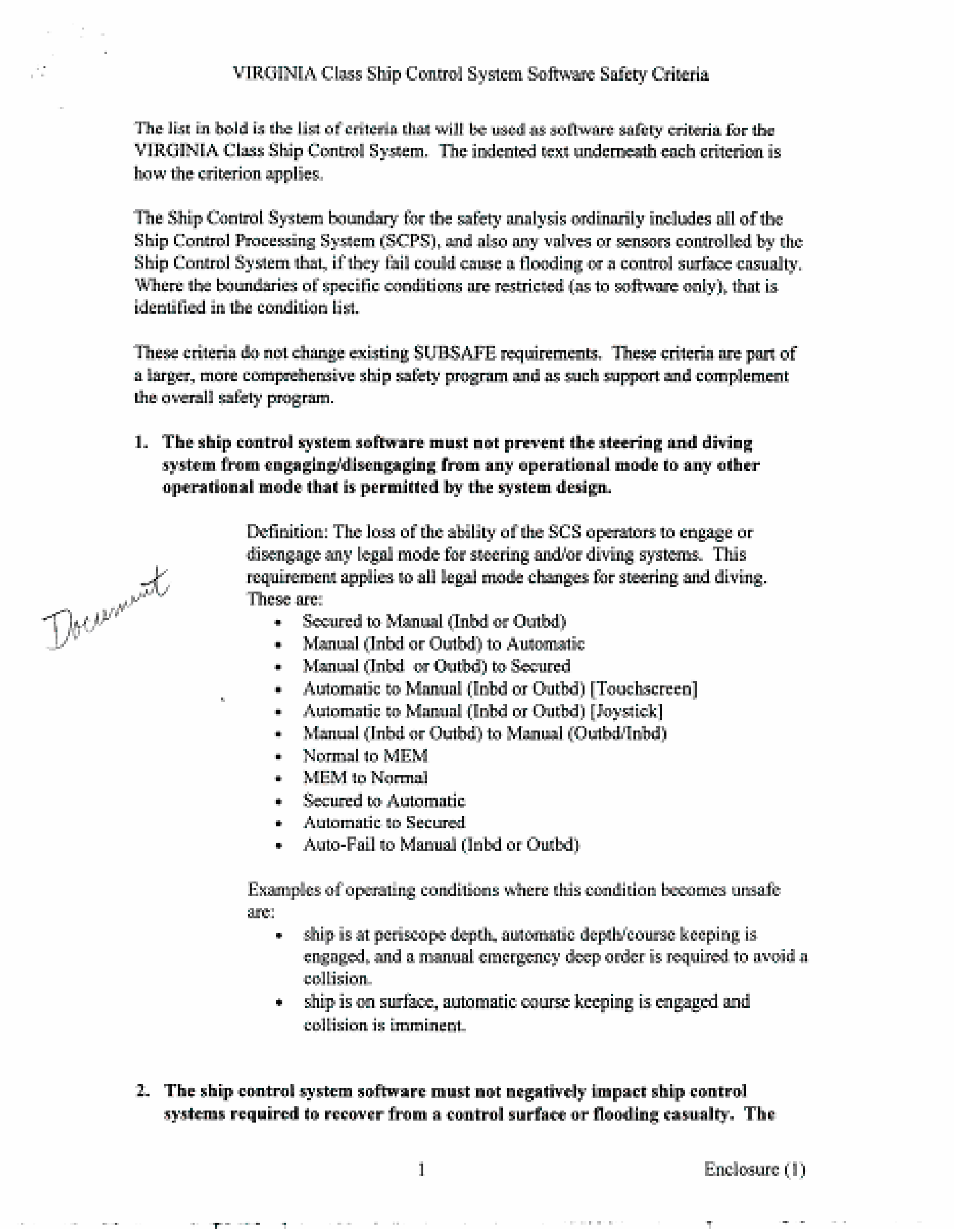
CONCURRENCE:

PMS450 ____ 11/6/98

SEA 03U John T. Leadmon 11/6/98

RECORD NOTE:

1. This letter forwards the final system level NSSN Ship Control System Software Safety Criteria for use in software code development. At a meeting between NAVSEA and EB representatives in June 1998, EB presented their interpretation of the safety criteria that SEA 03J2 provided EB in January of 1998. Based on the EB interpretation, NAVSEA realized the safety criteria needed adjustment. The finalized safety criteria reflects this adjustment.



VIRGINIA Class Ship Control System Software Safety Criteria

The list in bold is the list of criteria that will be used as software safety criteria for the VIRGINIA Class Ship Control System. The indented text underneath each criterion is how the criterion applies.

The Ship Control System boundary for the safety analysis ordinarily includes all of the Ship Control Processing System (SCPS), and also any valves or sensors controlled by the Ship Control System that, if they fail could cause a flooding or a control surface casualty. Where the boundaries of specific conditions are restricted (as to software only), that is identified in the condition list.

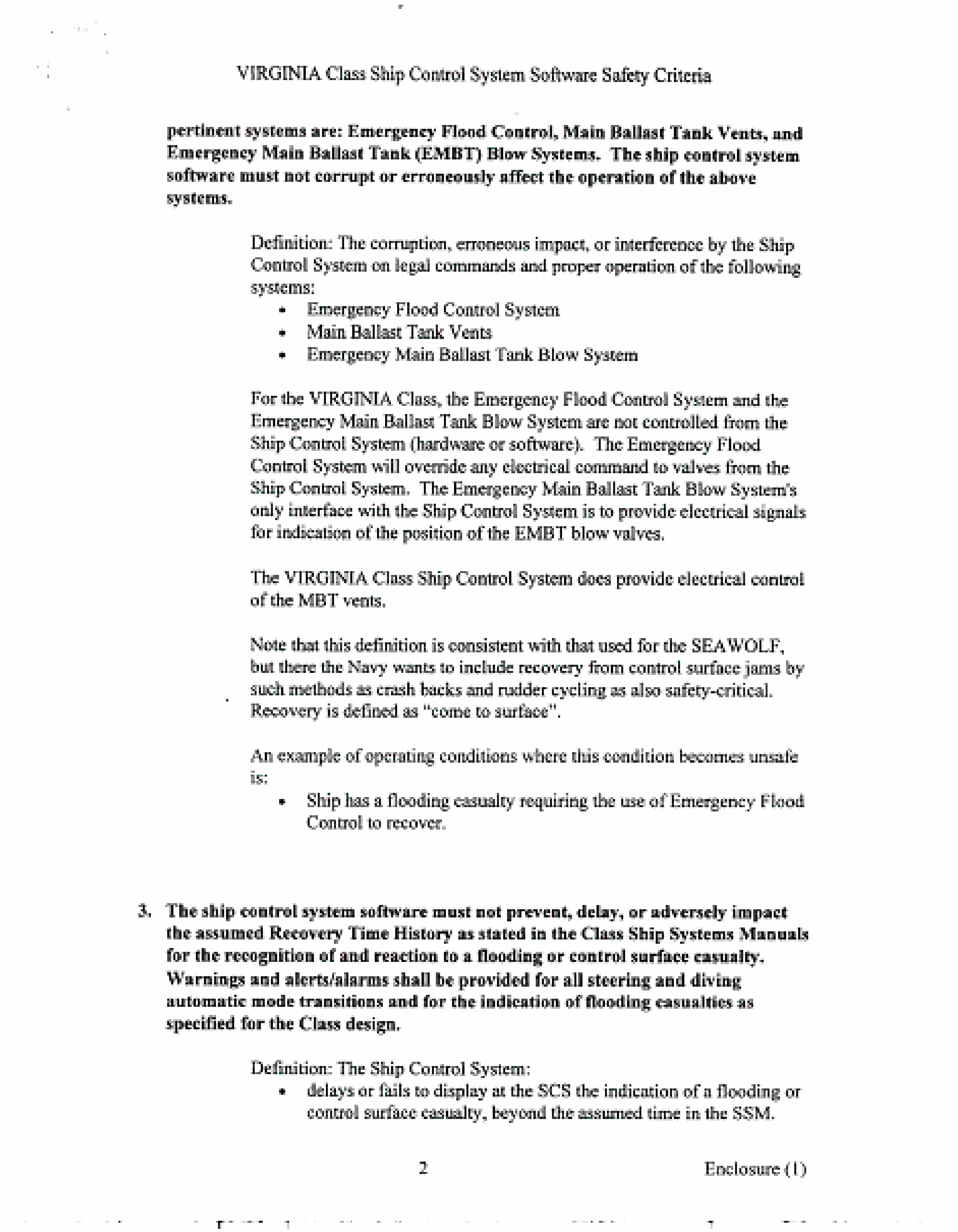
These criteria do not change existing SUBSAFE requirements. These criteria are part of a larger, more comprehensive ship safety program and as such support and complement the overall safety program.

1. **The ship control system software must not prevent the steering and diving system from engaging/disengaging from any operational mode to any other operational mode that is permitted by the system design.**

Document

> Definition: The loss of the ability of the SCS operators to engage or disengage any legal mode for steering and/or diving systems. This requirement applies to all legal mode changes for steering and diving. These are:
>
> - Secured to Manual (Inbd or Outbd)
> - Manual (Inbd or Outbd) to Automatic
> - Manual (Inbd or Outbd) to Secured
> - Automatic to Manual (Inbd or Outbd) [Touchscreen]
> - Automatic to Manual (Inbd or Outbd) [Joystick]
> - Manual (Inbd or Outbd) to Manual (Outbd/Inbd)
> - Normal to MEM
> - MEM to Normal
> - Secured to Automatic
> - Automatic to Secured
> - Auto-Fail to Manual (Inbd or Outbd)
>
> Examples of operating conditions where this condition becomes unsafe are:
>
> - ship is at periscope depth, automatic depth/course keeping is engaged, and a manual emergency deep order is required to avoid a collision.
> - ship is on surface, automatic course keeping is engaged and collision is imminent.

2. **The ship control system software must not negatively impact ship control systems required to recover from a control surface or flooding casualty. The**



pertinent systems are: Emergency Flood Control, Main Ballast Tank Vents, and Emergency Main Ballast Tank (EMBT) Blow Systems. The ship control system software must not corrupt or erroneously affect the operation of the above systems.

Definition: The corruption, erroneous impact, or interference by the Ship Control System on legal commands and proper operation of the following systems:

- Emergency Flood Control System
- Main Ballast Tank Vents
- Emergency Main Ballast Tank Blow System

For the VIRGINIA Class, the Emergency Flood Control System and the Emergency Main Ballast Tank Blow System are not controlled from the Ship Control System (hardware or software). The Emergency Flood Control System will override any electrical command to valves from the Ship Control System. The Emergency Main Ballast Tank Blow System's only interface with the Ship Control System is to provide electrical signals for indication of the position of the EMBT blow valves.

The VIRGINIA Class Ship Control System does provide electrical control of the MBT vents.

Note that this definition is consistent with that used for the SEAWOLF, but there the Navy wants to include recovery from control surface jams by such methods as crash backs and rudder cycling as also safety-critical. Recovery is defined as "come to surface".

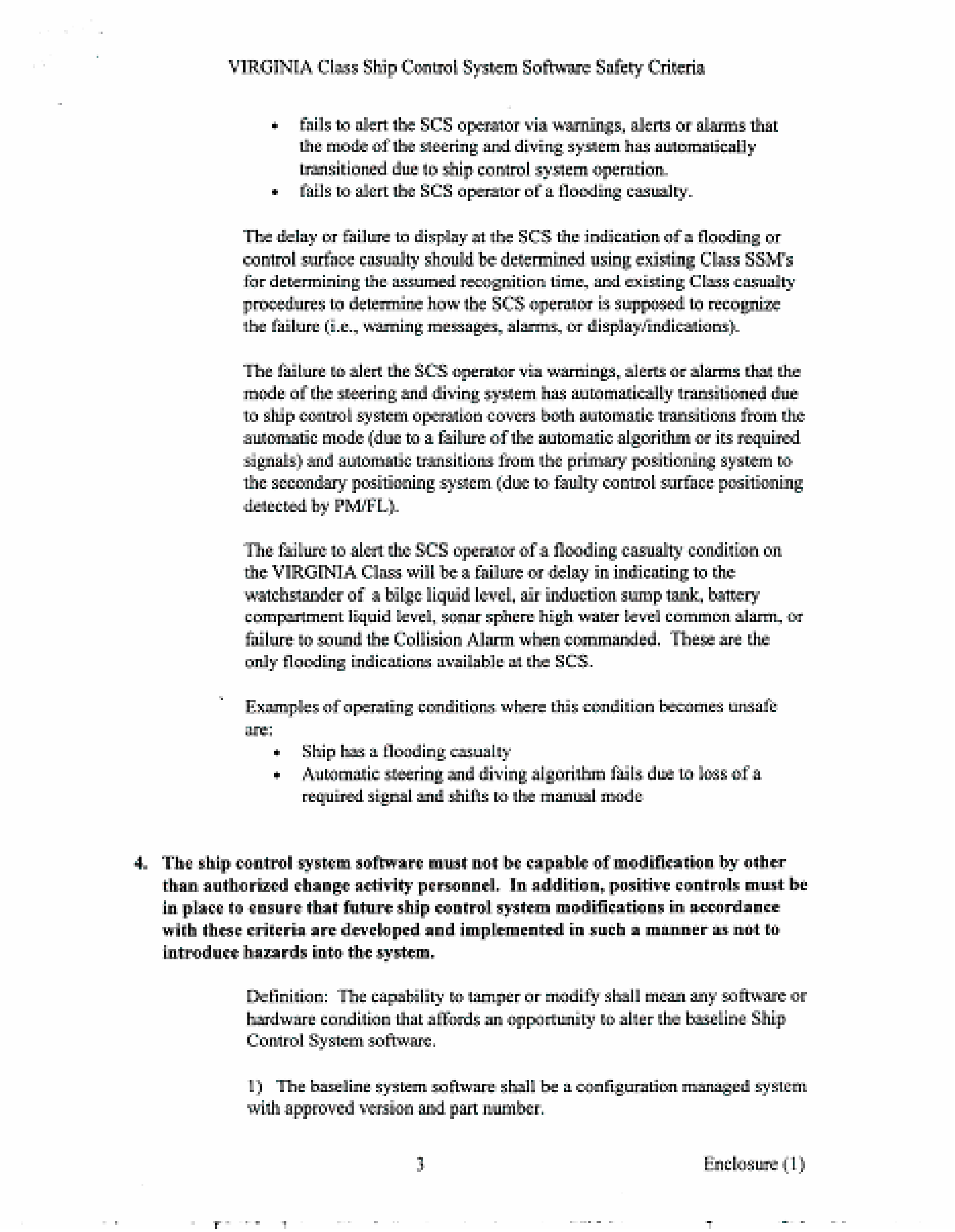
An example of operating conditions where this condition becomes unsafe is:

- Ship has a flooding casualty requiring the use of Emergency Flood Control to recover.

3. **The ship control system software must not prevent, delay, or adversely impact the assumed Recovery Time History as stated in the Class Ship Systems Manuals for the recognition of and reaction to a flooding or control surface casualty. Warnings and alerts/alarms shall be provided for all steering and diving automatic mode transitions and for the indication of flooding casualties as specified for the Class design.**

Definition: The Ship Control System:

- delays or fails to display at the SCS the indication of a flooding or control surface casualty, beyond the assumed time in the SSM.



- fails to alert the SCS operator via warnings, alerts or alarms that the mode of the steering and diving system has automatically transitioned due to ship control system operation.
- fails to alert the SCS operator of a flooding casualty.

The delay or failure to display at the SCS the indication of a flooding or control surface casualty should be determined using existing Class SSM's for determining the assumed recognition time, and existing Class casualty procedures to determine how the SCS operator is supposed to recognize the failure (i.e., warning messages, alarms, or display/indications).

The failure to alert the SCS operator via warnings, alerts or alarms that the mode of the steering and diving system has automatically transitioned due to ship control system operation covers both automatic transitions from the automatic mode (due to a failure of the automatic algorithm or its required signals) and automatic transitions from the primary positioning system to the secondary positioning system (due to faulty control surface positioning detected by PM/FL).

The failure to alert the SCS operator of a flooding casualty condition on the VIRGINIA Class will be a failure or delay in indicating to the watchstander of a bilge liquid level, air induction sump tank, battery compartment liquid level, sonar sphere high water level common alarm, or failure to sound the Collision Alarm when commanded. These are the only flooding indications available at the SCS.

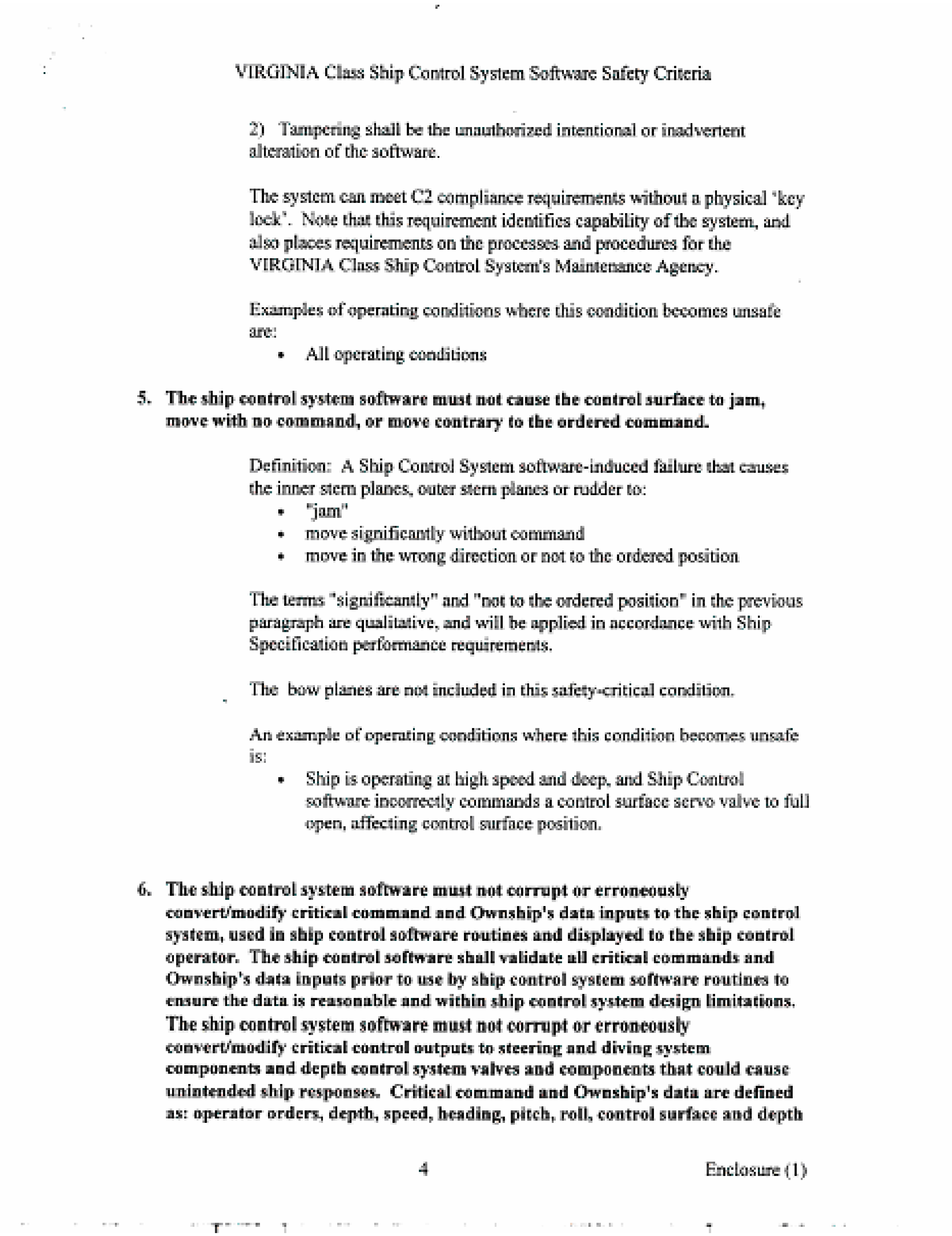
Examples of operating conditions where this condition becomes unsafe are:

- Ship has a flooding casualty
- Automatic steering and diving algorithm fails due to loss of a required signal and shifts to the manual mode

4. The ship control system software must not be capable of modification by other than authorized change activity personnel. In addition, positive controls must be in place to ensure that future ship control system modifications in accordance with these criteria are developed and implemented in such a manner as not to introduce hazards into the system.

Definition: The capability to tamper or modify shall mean any software or hardware condition that affords an opportunity to alter the baseline Ship Control System software.

1) The baseline system software shall be a configuration managed system with approved version and part number.



2) Tampering shall be the unauthorized intentional or inadvertent alteration of the software.

The system can meet C2 compliance requirements without a physical 'key lock'. Note that this requirement identifies capability of the system, and also places requirements on the processes and procedures for the VIRGINIA Class Ship Control System's Maintenance Agency.

Examples of operating conditions where this condition becomes unsafe are:

- All operating conditions

5. **The ship control system software must not cause the control surface to jam, move with no command, or move contrary to the ordered command.**

Definition: A Ship Control System software-induced failure that causes the inner stern planes, outer stern planes or rudder to:

- "jam"
- move significantly without command
- move in the wrong direction or not to the ordered position

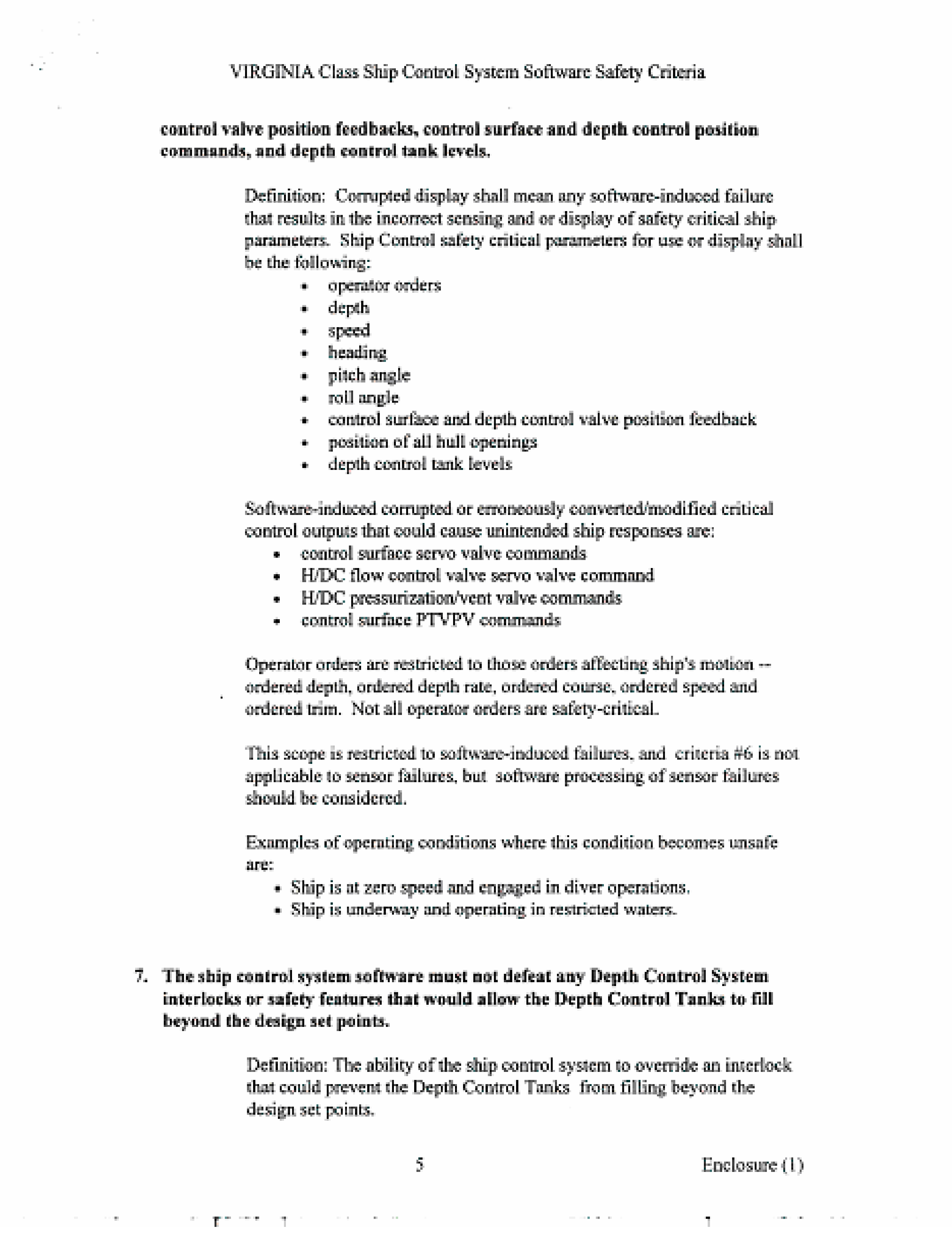
The terms "significantly" and "not to the ordered position" in the previous paragraph are qualitative, and will be applied in accordance with Ship Specification performance requirements.

The bow planes are not included in this safety-critical condition.

An example of operating conditions where this condition becomes unsafe is:

- Ship is operating at high speed and deep, and Ship Control software incorrectly commands a control surface servo valve to full open, affecting control surface position.

6. **The ship control system software must not corrupt or erroneously convert/modify critical command and Ownship's data inputs to the ship control system, used in ship control software routines and displayed to the ship control operator. The ship control software shall validate all critical commands and Ownship's data inputs prior to use by ship control system software routines to ensure the data is reasonable and within ship control system design limitations. The ship control system software must not corrupt or erroneously convert/modify critical control outputs to steering and diving system components and depth control system valves and components that could cause unintended ship responses. Critical command and Ownship's data are defined as: operator orders, depth, speed, heading, pitch, roll, control surface and depth**



control valve position feedbacks, control surface and depth control position commands, and depth control tank levels.

Definition: Corrupted display shall mean any software-induced failure that results in the incorrect sensing and or display of safety critical ship parameters. Ship Control safety critical parameters for use or display shall be the following:

- operator orders
- depth
- speed
- heading
- pitch angle
- roll angle
- control surface and depth control valve position feedback
- position of all hull openings
- depth control tank levels

Software-induced corrupted or erroneously converted/modified critical control outputs that could cause unintended ship responses are:

- control surface servo valve commands
- H/DC flow control valve servo valve command
- H/DC pressurization/vent valve commands
- control surface PTVPV commands

Operator orders are restricted to those orders affecting ship's motion -- ordered depth, ordered depth rate, ordered course, ordered speed and ordered trim. Not all operator orders are safety-critical.

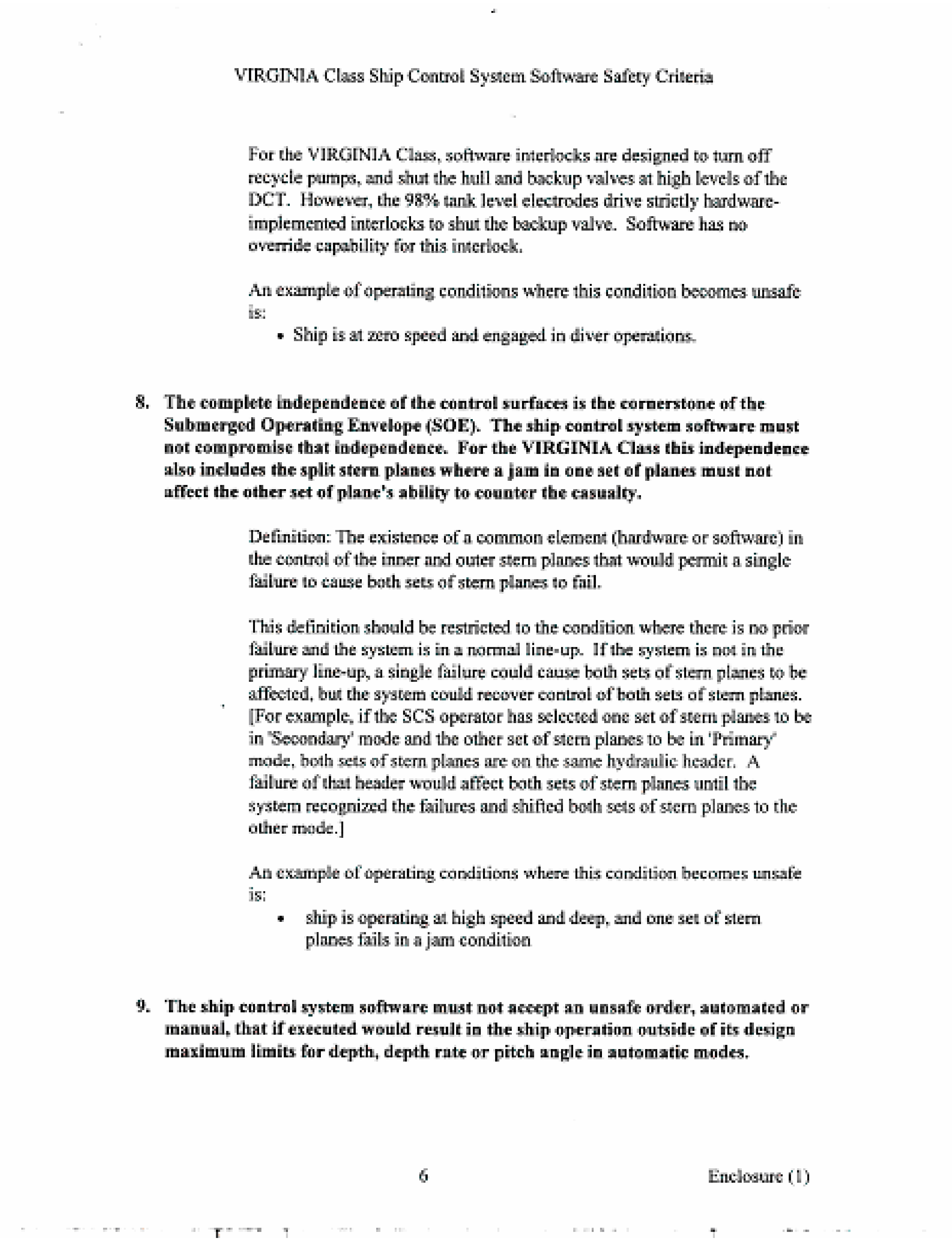
This scope is restricted to software-induced failures, and criteria #6 is not applicable to sensor failures, but software processing of sensor failures should be considered.

Examples of operating conditions where this condition becomes unsafe are:

- Ship is at zero speed and engaged in diver operations.
- Ship is underway and operating in restricted waters.

7. **The ship control system software must not defeat any Depth Control System interlocks or safety features that would allow the Depth Control Tanks to fill beyond the design set points.**

Definition: The ability of the ship control system to override an interlock that could prevent the Depth Control Tanks from filling beyond the design set points.



For the VIRGINIA Class, software interlocks are designed to turn off recycle pumps, and shut the hull and backup valves at high levels of the DCT. However, the 98% tank level electrodes drive strictly hardware-implemented interlocks to shut the backup valve. Software has no override capability for this interlock.

An example of operating conditions where this condition becomes unsafe is:

- Ship is at zero speed and engaged in diver operations.

8. **The complete independence of the control surfaces is the cornerstone of the Submerged Operating Envelope (SOE). The ship control system software must not compromise that independence. For the VIRGINIA Class this independence also includes the split stern planes where a jam in one set of planes must not affect the other set of plane's ability to counter the casualty.**

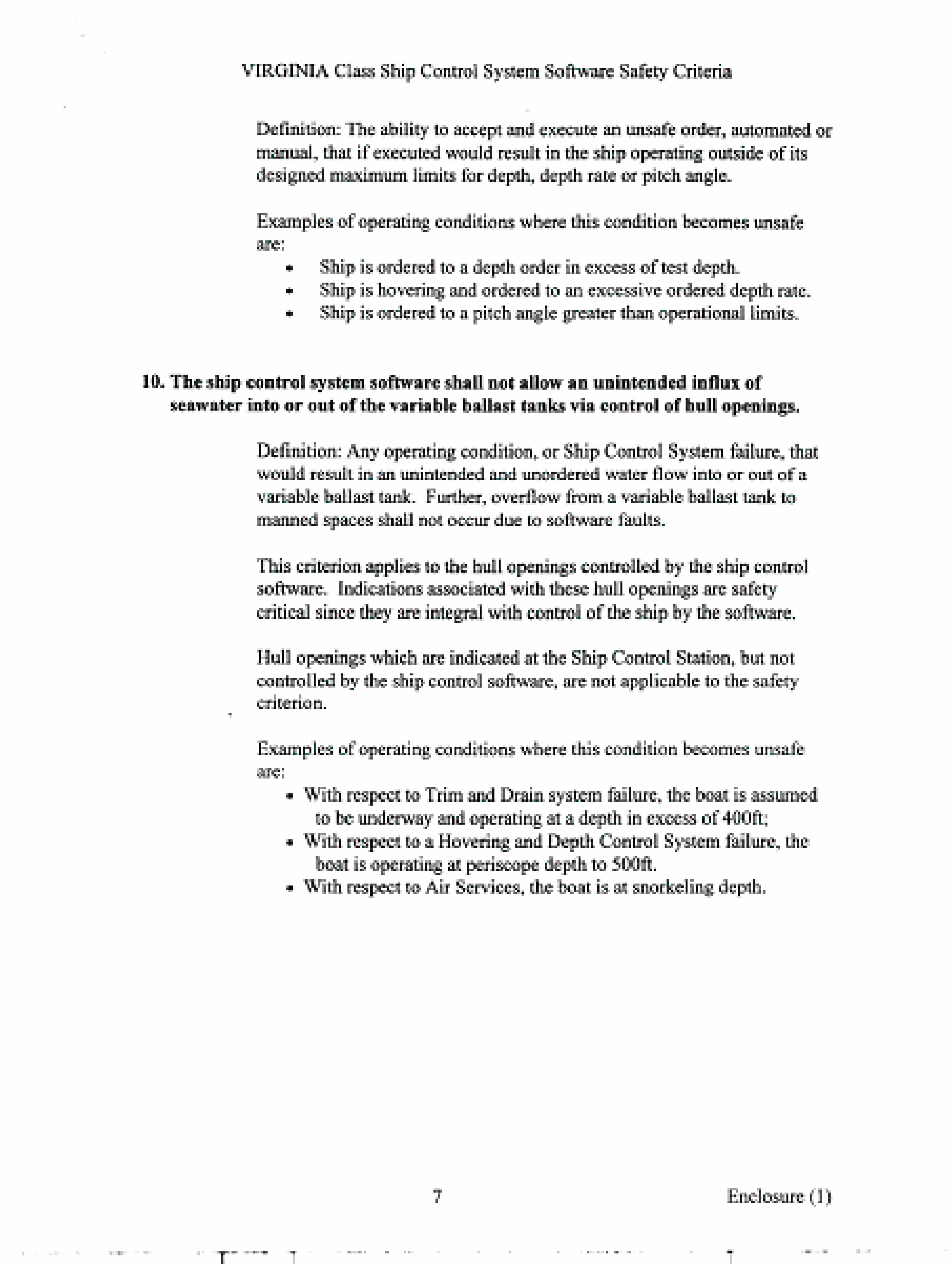
Definition: The existence of a common element (hardware or software) in the control of the inner and outer stern planes that would permit a single failure to cause both sets of stern planes to fail.

This definition should be restricted to the condition where there is no prior failure and the system is in a normal line-up. If the system is not in the primary line-up, a single failure could cause both sets of stern planes to be affected, but the system could recover control of both sets of stern planes. [For example, if the SCS operator has selected one set of stern planes to be in 'Secondary' mode and the other set of stern planes to be in 'Primary' mode, both sets of stern planes are on the same hydraulic header. A failure of that header would affect both sets of stern planes until the system recognized the failures and shifted both sets of stern planes to the other mode.]

An example of operating conditions where this condition becomes unsafe is:

- ship is operating at high speed and deep, and one set of stern planes fails in a jam condition

9. **The ship control system software must not accept an unsafe order, automated or manual, that if executed would result in the ship operation outside of its design maximum limits for depth, depth rate or pitch angle in automatic modes.**



Definition: The ability to accept and execute an unsafe order, automated or manual, that if executed would result in the ship operating outside of its designed maximum limits for depth, depth rate or pitch angle.

Examples of operating conditions where this condition becomes unsafe are:

- Ship is ordered to a depth order in excess of test depth.
- Ship is hovering and ordered to an excessive ordered depth rate.
- Ship is ordered to a pitch angle greater than operational limits.

10. The ship control system software shall not allow an unintended influx of seawater into or out of the variable ballast tanks via control of hull openings.

Definition: Any operating condition, or Ship Control System failure, that would result in an unintended and unordered water flow into or out of a variable ballast tank. Further, overflow from a variable ballast tank to manned spaces shall not occur due to software faults.

This criterion applies to the hull openings controlled by the ship control software. Indications associated with these hull openings are safety critical since they are integral with control of the ship by the software.

Hull openings which are indicated at the Ship Control Station, but not controlled by the ship control software, are not applicable to the safety criterion.

Examples of operating conditions where this condition becomes unsafe are:

- With respect to Trim and Drain system failure, the boat is assumed to be underway and operating at a depth in excess of 400ft;
- With respect to a Hovering and Depth Control System failure, the boat is operating at periscope depth to 500ft.
- With respect to Air Services, the boat is at snorkeling depth.

Glossary

ADARTS	Ada Design Approach for Real Time Systems
AHP	Analytical Hierarchy Process
AIS	Automated Information System
Ao	Operational Availability
API	Application Interfaces
APPL	NASA Academy of Program and Project Leadership
ARCI	Automatic Rapid COTS Insertion
ASAP	Aerospace Safety Advisory Panel
ASDS	Advanced Seal Delivery System
BFS	Backup Flight System
BIOS	Basic Input/Output System
C3I	Command, Control, Communications, and Intelligence
CAGE	Commercial And Government Entity code -- a five-digit code that identifies companies doing or planning to do business with the federal government
CAIB	Columbia Accident Investigation Board
CASREP	Casualty Report
CAU	Cockpit Avionics Upgrade
CCB	Configuration Control Board
CDR	Critical Design Review
Cert PAT	Certification Process Action Team
CFE	Contractor Furnished Equipment
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CLCS	Checkout and Launch Control System
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integrated
COFR	Certification of Flight Readiness
COOPEX	Concept of Operations Exercise
COTS	Commercial Off-the-Shelf
CPU	Central Processing Unit

CRE	Certified Reliability Engineer
CSCI	Computer Software Configuration Items
CSP	Certified Safety Professional
DLA	Defense Logistics Agency
DMP	Depot Maintenance Period
DSS	Deep Submergence Systems
EB	Electric Boat (General Dynamics, Electric Boat Division)
ERO	Engineering Refueling Overhaul
FBW	Fly-by-Wire
FCA	Functional Configuration Audits
FMEA	Failure Modes and Effects Analysis
FRR	Flight Readiness Review
FSC	Federal Stock Classification
FTA	Fault Tree Analysis
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GIDEP	Government-Industry Data Exchange Program
GPMC	Governing Program Management Council
HF FMEA	Human Factors FMEA
HM&E	Hull, Mechanical, and Electrical
HMF	Hypergolic Maintenance Facility
HP	Hewlett Packard
HWCI	Hardware Configuration Item
IA	Independent Assessment
IBM FSD	IBM Federal Systems Division
ICD	Initial Capability Document
IDS	Interface Design Specifications
IDS CCB	Integrated Data Systems Change Control Board
IEEE	Institute of Electrical and Electronic Engineers
ILS	Integrated Logistics Support
INSRV	In Service
IPA	In Process Audit
IPAO	Internal Process Assessments Office

IPPD	Integrated Product and Process Development
IPT	Integrated Product Team
IRS	Interface Requirements Specifications
IRT	Interface Requirements Table
ISS	International Space Station
ITMP	Individual Task Management Plan
IV&V	Independent Verification and Validation
JSC	Johnson Space Center
JSSC	Joint Services Safety Certification
KAPL	Knolls Atomic Power Laboratory
KATS	Kennedy Avionics Test Set
KSC	Kennedy Space Center
LPS	Launch Processing System
MAUT	Multi-Attribute Utility Theory
MMT	Manned Mission Team (RTF)
MOA	Memorandum of Agreement
NASA	National Aeronautics and Space Administration
NASDA	National Space Development Agency
NAVSEA	Naval Sea Systems Command
NAVSEALOGCENDET	Naval Sea Logistics Center Detachment
NAWC	Naval Air Warfare Center
NDT	Non destructive Test
NEQA	NASA Engineering and Quality Audits
NESC	NASA Engineering and Safety Center
NNBE	NASA/Navy Benchmarking Exchange
NNPP	Naval Nuclear Propulsion Program
NPD	NASA Policy Directive
NPES	Non-Propulsion Electronic System
NPG	NASA Procedure and Guideline
NPR	NASA Procedural Requirements
NR	Naval Reactors
NSWC	Naval Surface Warfare Center
NUWC	Naval Undersea Warfare Center

OPF	Orbiter Processing Facility
OPTEVFOR	Operational Test and Evaluation Force
OQE	Objective Quality Evidence
ORD	Operational Requirements Document
OSMA	Office of Safety and Mission Assurance
PAR	Preliminary Acceptance Review
PASS	Primary Avionics Software System
PCA	Physical Configuration Audits
PCGOAL	Personal Computer Ground Operations Aerospace Language *(Note: PCGOAL is a legacy name which describes a group of computers used to maintain the Shuttle Data Stream during flight. The platform is not actually built on the GOAL language.)*
PDR	Preliminary Design Review
PDREP	Product Data Reporting and Evaluation Program
PEO	Program Executive Officer
PEO SUB	Program Executive Officer, Submarines
PHA	Preliminary Hazard Analysis
PHNSY&IMF	Pearl Harbor Naval Shipyard & Intermediate Maintenance Facility
PIDS	Prime Item Development Specifications
PM	Program Manager
PSRP	Payload Safety Review Panel
PTR	Program Trouble Report
PV	Process Verification
R&D	Research and Development
RAM	Risk Area Manager
RDT&E	Research, Development, Test and Evaluation
RFP	Request for Proposal
Rm	Mission Reliability
ROI	Return on Investment
RTF	Return to Flight
RYG	Red/Yellow/Green
SA	Software Assurance

SAIL	Shuttle Avionics Integration Lab
SASCB	Shuttle Avionics Software Control Board
SAWG	Software Assurance Working Group
SCDM	Safety Critical Decision Making (Training Initiative)
SCS	Ship Control System
SDDD	Software Detailed Design Documents
SEI	Software Engineering Institute
SIT	System Integration Team
SLEP	Shuttle Life Extension Program
SMA	Safety and Mission Assurance
SME	Subject Matter Expert
SPMN	Software Program Managers Network
SPRDE	Systems Planning, Research, Development, and Engineering
SRS	Software Requirements Specifications
SSC	Submarine Safety Collo1quium
SSDD	Ship Safety Description Document
SSMEC	Space Shuttle Main Engine Control
SSP	Space Shuttle Program
SSSTRP	Software System Safety Technical Review Panel
SUBSAFE	Submarine Safety Program
SUPSHIPS	Supervisor of Shipbuilding
TADSTANDS	Tactical Digital Standards
USA	United Space Alliance (Lockheed Martin and Boeing)
VPP	Voluntary Protection Program
WSESRB	Weapon System Explosives Safety Review Board

Referenced Documents

CJCSI 3170.01D – Joint Capabilities Integration and Development System, Chairman of the Joint Chiefs of Staff Instruction

DOD-STD-2167A (Canceled) – Defense System Software Development

DOD-STD-2168 (Canceled) – Defense System Software Quality Program

DoD 5000 Series – Comprised of DoD Directive 5000.1, The Defense Acquisition System, and DoD Instruction 5000.2, Operation of the Defense Acquisition System

IEEE/EIA 12207 – Industry implementation of ISO/IEC 12207, "Software Life Cycle Processes."

ISO 9000:2000 – *Quality management systems - Fundamentals and vocabulary* (December 13, 2000

ISO 9001:2000 – *Quality management systems - Requirements* (December 13, 2000), contains the requirements for a QMS. This Manual (QA01) is basically a "customized" version of 9001:2000.

ISO 9004:2000 – *Quality management systems - Guidelines For Performance Improvements* (December 13, 2000), contains guidelines (not requirements) for an organization's QMS effectiveness and efficiency, leading to improvements in performance and customer satisfaction.

MIL-STD-498 (Canceled) – Software Development and Documentation

MIL-STD-882C – System Safety Program Requirements

MIL-STD-973 (Canceled) – Configuration Management

NAVSEAINST 4855.35 – NAVSEA Submarine Safety (SUBSAFE) Functional Audit Program

NPR 8715.3 – NASA Safety Manual w/Change 2, 03/31/04

STANAG 4404 (Draft) – NATO Standardization Agreement (STANAG), Safety Design Requirements and Guidelines for Munitions Related Safety Critical Computing Systems.